BID DOCUMENT

For

Development of Campus Wide Digital Network Solutions and Services For New Blocks At Masjid Moth, AIIMS New Delhi and NCI Jhajjar

VOLUME – IV

Technical Specifications

April- 2018

ह.स.कं.क.
HSCC

CONSULTANT
HSCC (INDIA) LTD
E-6(A), Sector-1, NOIDA(U.P) 201301 (India)
Phone: 0120-2542436-40 Fax: 0120-2542447

Tender No: - HSCC/AIIMS/IT/2018

1 Scope of Work

1. Establishment of Campus Wide Digital Network Solutions and Services For New Blocks(New OPD Block, Surgical Specialties Block, Mother & Child Block) At Masjid Moth, AIIMS, New Delhi and (National Cancer Institute) NCI, Jhajjar, Haryana

2. Supply, Installation, Configuration, Commissioning and Maintenance of LAN & Wi-Fi network as per the requirement of Institute and scope of work mentioned.

   LAN & Wi-Fi shall be used for running HMIS, PACS, Access control systems for Biometric Attendance System, Patient Access System through scanning, display system including outside OPD / Consultant rooms, Common rooms Hall etc., Public Address System, Internal Telemedicine (Video Conferencing), Queue Management System, CCTV, traffic and parking management & Other applications. Complete IT system i.e. Network Infrastructure Solutions and Services (LAN & Wi-Fi) should be fully functional in all respects and to the satisfaction of the AIIMS.

3. Establishment of Data centre to cater to the requirements of the campus at AIIMS, New Delhi and NCI Jhajjar. (One Data centre for NCI, One Data Centre for AIIMS New Delhi)

4. Operation, maintenance & Support for IT Networking services including provision of necessary on-site technical support as per requirements.

5. Set-up on-site 24x7 Help desks for all types of help & support for operation & maintenance of IT infrastructure Solutions and Services.

6. Complete Network Infrastructure Solutions and Services shall be provided with 5 years onsite comprehensive warranty and subsequent 5 years Comprehensive Maintenance Support from 6th to 10th years (if awarded) including labour, spares, accessories and consumables.

7. Any other related work as per the requirement of the Institute.

2 Introduction

1. The AIIMS New Delhi has plan to set-up information technology infrastructure Solutions and Services for New OPD block, Surgical Block, Mother and Child Block at Masjid Moth campus, AIIMS, New Delhi and New blocks at NCI, Jhajjar to efficiently provide high quality state-of-the-art medical care by creating a modern streamlined professional work environment for medical, nursing and allied professionals.
2. All the upcoming blocks at Masjid Moth campus, AIIMS, New Delhi and NCI Jhajjar have rooms ear-marked for Consultant, Residents, OPD Rooms, Waiting rooms etc. The services & facilities include X-Ray, Ultrasound, ECG, Blood Sample Collection, Endoscopy & Pharmacy.
3. New OPD block has 500 plus consultant Rooms, conference rooms, pharmacy, etc. The services & facilities include X-Ray, Ultrasound, ECG, Blood Sample Collection, Endoscopy & Pharmacy. It has capacity to cater more than 10000 patients per day.
4. Mother & Child Block has 12 floors including 3 Basements, Ground and Eight floors. It has bed capacity of 400 Beds. Services & facilities includes consultant rooms, X-ray, CSSD, CT-Scan, Ultrasound, Control room, Reporting room, Reception, Registration, Modular OTs, OT store, TSSUs, HDUs, LAB, Medical Gas Manifold System, Kitchen, Laundry, Bio-Medical Waste Management System, Private Rooms etc.
5. Surgical Block has 12 floors including 3 Basements, Ground and Eight floors. It has bed capacity of 200 beds. The services and facilities includes Helpdesk, Registration, Investigation (X-Ray, CT-Scan, Ultra-Sound, Mammography), Minor OT, Pre-OP, Post-OP, Store, Wards, Nurse stations, Consultant rooms, Laparoscopy, Laboratories, ICUs, HDUs, OTs, TSSUs, Laundry, CSSD, Medical Gas Manifold System, Blood Bank, Canteen, Server room etc.
6. NCI has 7 major blocks and residential complex. It has bed capacity of 710 Beds. Services & facilities includes consultant rooms, X-ray, CSSD, CT-Scan, Ultrasound, Control room, Reporting room, Reception, Registration, Modular OTs, OT store, TSSUs, HDUs, LAB, Medical Gas Manifold System, Kitchen, Laundry, Bio-Medical Waste Management System, Private Rooms etc.

7. As these are new blocks at AIIMS Masjid Moth & NCI Jhajjar campus, Institute wishes to setup a State-of- the-Art, high performance, fault-tolerant, secure and highly available IT & Networking (LAN & Wi-Fi) infrastructure solution and shall utilize the best of products and the latest, open standards based technology, high quality services and workmanship.
8. Proposed Network Point details for all the blocks at AIIMS, New Delhi and NCI Jhajjar-

New OPD Block	:	3B+G+8Floors, 3000 Network Nodes
Surgical Block	:	3B+G+8Floors, 800 Network Nodes
Mother & Child Block	:	3B+G+8Floors, 2000 Network Nodes
NCI Jhajjar	:	7 Buildings and 4-6 Hostels, 8000 Network Nodes

3 Planned Facilities at New OPD Block at AIIMS, New Delhi

- The central spine has provisions for service shafts, drinking water wheel chair alcoves / disposal systems etc.
- 3B+G+8 floors for OPDs
- Total Rooms - 530
- Load at 20 lakh /annum = 10,000 per day (provided for)
- 800 -1000 seating on each floor

4 Planned Facilities at Mother and Child at AIIMS, New Delhi

Hospital Infrastructure

1. Day Care -100 beds
2. Ward -77 beds
3. Isolation -12 beds
4. Room – 142 beds
5. Ward (HDU) -26 beds
6. Pre. -Operative 20 beds
7. Post -operative – 12 beds
8. Triage -3 beds

(Total approx. Beds -400 beds)

System and Services

1. Modular Operation Theatres
2. Central Sterile Supply Department (CSSD)
3. Medical Gases Manifold System
4. Kitchen
5. Laundry
6. Bio- Medicals Waste Management System

FLOOR	
Basement- Level-1	OPD expansion, Consultant room, X-ray,C.S.S.D., CT Scan
Basement- Level-2	Car Parking
Basement- Level-3	Car Parking
Ground Floor	X-Ray, Ultrasound, Control Room, Reporting Room, Reception, Registration, Consultant room
1st Floor	Operation Theatres, Pre & Post Operative, OT store, Ultrasound, Nursary, Delivery suit
2nd Floor	Admin Office, Day care, Operation Theatres, Pre & Post Operative, Doctor's Change Rooms,Theatre steralize supply unit, T.S.S.U.
3rd Floor	Private Rooms, Wards, Support Facilities
4th Floor	Private Rooms, Wards, Support Facilities
5th Floor	Private Rooms, Day care, HDU, Isolation Ward
6th Floor	Day care, HDU, Isolation Ward
7th Floor	Admin offic , LAB, Lecture hall
8th Floor	LAB, Lecture hall

Total Bed Distribution

Description	**No. of Beds**
Triage Beds	3
Ward Beds	77
Pre & Post Operatives	32
Day Care	100
Room	142
Ward (HDU)	26
Isolation Ward	12

Tentative Radiology services for PACS

Radiology Information	**Quantity**
X-Ray	3 nos.
Ultrasound	4 nos.
CT scan	1 nos.

5 Planned Facilities at Surgical Block at AIIMS, New Delhi

Infrastructure Details

- 3 Basements + Ground floor + 8 floors
- Area – 22000 Sq. M.
- Bed Capacity – 200 Beds
- No. of Operation Theatres – 12
- ICU – 13, HDU – 12

Floor –wise details

Floor	Details
Basement-III	Car Parking
Basement-II	Car Parking
Basement-I	Laundry, Canteen, CSSD
Ground Floor	Registration, Help Desk, Investigation Area (X-Ray, CT-Scan, Ultra-Sound, Mammography), Minor OT, Pre-OP, Post-OP
First Floor	Store, Wards, Nurse Stations
Second Floor	Store, Wards, Nurse Stations
Third Floor	Store, Wards, Nurse Stations
Fourth Floor	Consultants Room(37), Laparoscopy
Fifth Floor	Laboratories(2), ICU(13), Transplantation Ward(10), HDU(12)
Sixth Floor	OT(6), TSSU, Store
Seventh Floor	OT(6), TSSU, Store
Eighth Floor	Server Room

Tentative Major Radiology Equipments:

- MRI 3.5 Tesla – 1 no.
- CT Scan - 1 no.
- Ultrasound with Color Doppler - 1 no.
- Imaging X- Ray Machine for Mammography - 1 no.
- Imaging X- Ray Machine 1000 Ma Machine, Ceiling Suspended - 1 no.
- Imaging X- Ray Machine(Mobile) 100 ma HF – 8 no
- Imaging Ultrasound Machine Sector scanning, with two Probes – 1 no.
- Imaging C- Arm Mobile X-Ray Machine with viewing console with two monitors – 3 no.

6 Planned Facilities for National Cancer Institute (NCI) at Jhajjar

The infrastructure details of NCI Jhajjar is as follows:

Block	No. Of Floors
Basic Science Research Block	Ground + 5
PC Teaching Block	Ground + 3

Admin Block	Ground + 6
OPD Block	Ground + 4
Hospital Block	Basement + Ground + 8
Clinical Research	Ground + 6
Residential Campus	Multiple building

Departments

- Surgical Oncology
- Radiation Oncology
- Medical Oncology
- Anaesthesia and Palliative care
- Nuclear Medicine

Clinical Divisions:

- Surgical Oncology
- Radiation Oncology
- Medical Oncology
- Radiology
- Nuclear Medicine
- Tumor Patho-biology
- Lab medicine
- Anesthesiology and Hospice
- Preventive Oncology
- Medical Physics
- Hospital administration
- Psycho-oncology
- Palliative care & Hospice
- Blood bank
- Emergency
- Physiotherapy &Occupational Therapy

Research Divisions:

- Bioethics & Bio-safety Division
- Cancer Epidemiology
- Molecular Oncology
- Cancer Genomics & Proteomics
- Cancer Vaccine & Immunotherapy
- Drug designing & Drug development
- Development of Medical tools & Diagnostics
- Pharmaco-genonics & Drug Discovery
- Occupational Cancer Research
- Radiobiology & Radiation Research
- Human Resource Development in oncology
- Translational Research
- Biostatistics & Bioinformatics
- Animal House
- Tissue repository

SYSTEMS and SERVICES

The following Systems & Services play important roles in proper and efficient functioning of the Hospital.

- Modular Operation Theatre

- Central Sterile Supply Department (CSSD)
- Medical Gases Manifold System
- Kitchen
- Laundry
- Bio- Medicals Waste Management System
- Mortuary Chamber

Other Facilities:

- Basement Parking
- Service Zone
- Admin Block
- Housing
- Hostels
- Dharmshala/Night Shelter
- Plaza and interconnecting Sky Bridge

Departments	**Total beds proposed**
Surgical Oncology	**200**
Radiation Oncology	**120**
Medical Oncology	**200**
Anesthesia and Palliative Care	**60**
Nuclear Medicine	**20**
ICU beds	**50**
Emergency Beds	**30**
Day care beds	**30**
Total	**710**

7 Deliverables of the Project

The Project Plan/main deliverables, as a result of implementation of Network Solution (wired and Wi-Fi) at the New Blocks, shall address:

- Project Management Plan
- Pre-commissioning, Operational and User Acceptance Testing Plan
- Hardware Delivery and Installation Plan
- Network Design, Delivery and installation plan
- Training Plan
- Risk Management Plan
- Sustenance Plan
- Warranty Service Plan
- Task, Time, and Resource Schedules
- Post-Warranty Service Plan
- Technical Support Plan
- Quality Assurance and Control Process details which must include (but not limited to) detailing on Metrics, Reviews, Problem Reporting and Corrective action etc.
- Technical and Operational Process which must include (but not limited to) detailing on Methods, Tools, Techniques etc.
- Any other as per industries practice.

7.1 Network Solutions & Services

7.1.1 Establishment of Wired and Wi-fi Network

7.1.1.1 Detailed scope of work

1. The wired LAN and Wi-Fi networks are to be established for the New Blocks at both campus Masjid Moth, AIIMS, New Delhi and NCI Jhajjar.
2. The Networks of the above mentioned new Blocks should be integrated with existing network of AIIMS, New Delhi Campus.
3. The Local Area Network shall be established on 100G between Core switches, 40 Gigabit connectivity up to distribution switches (Network edge till core, core to distribution switch), and 10G connectivity between distribution to access switch and 1 G connectivity at Node Level. Core to Core 100G Connectivity.
4. The network shall be Optical Fiber upto Access switch & Cable Cat 6A thereafter (STP Cat 6A & Optical Fibre Cable). The connection between any two switches will be FOC. The cabling will be structured, and labeled. The conduits will run in a Tray.
5. In addition to the cable-based network, secured wireless network shall also be established for the above mentioned blocks and NCI Jhajjar.
6. The New OPD Block, Mother and Child Block and Surgical Block shall be connected to accessing AIIMS Network through FOC Connectivity as per following:
   a. 100G SM FOC Connectivity between New OPD block & Computer Facility, AIIMS, New Delhi.
   b. 40G SM FOC Connectivity between NOC 2 (near New Private Ward, AIIMS) and New OPD block.

   c. 40G SM FOC Connectivity between network of New OPD Block and CDER.
   d. 40G SM FOC Connectivity between Mother and Child block & Computer Facility.
   e. 40G SM FOC Connectivity between Mother and Child block & New OPD block.
   f. 40G SM FOC Connectivity between Surgical block & Computer Facility.
   g. 40G SM FOC Connectivity between Surgical block & New OPD block.

7. (The above mentioned FOC connectivity may change or increase as per the requirement of the Client at the time of commissioning)
8. All the New Blocks at NCI Jhajjar Campus shall be connected to Data Centre (DC1) at NCI Jhajjar Hospital Block 1st floor and at NCI Jhajjar Admin block 1st Floor (DC2) though SM FOC Connectivity as per following:
   a. Connectivity between network of OPD block to DC1 and DC2 as mentioned above through Min. 40 G FOC connectivity
   b. Connectivity between network of Academic block to DC1 and DC2 as mentioned above through Min. 40 G FOC connectivity
   c. Connectivity between network of Research block to DC1 and DC2 as mentioned above Through Min. 40 G FOC connectivity
   d. Connectivity between network of Guest House block to DC1 and DC2 as mentioned above Through Min. 40 G FOC connectivity
   e. Connectivity between network of Diagnostic block to DC1 and DC2 as mentioned above through Min. 40 G FOC connectivity
   f. Connectivity between network of Hospital block to DC1 and DC2 as mentioned above through Min. 40 G FOC connectivity
   g. Connectivity between network of Hospital block OT complex to DC1 and DC2 as mentioned above through Min. 40 G FOC connectivity
   h. Connectivity between network of Admin block to DC1 and DC2 as mentioned above through Min. 40 G FOC connectivity
   i. Connectivity between network of Residential Campus to DC1 and DC2 as mentioned above through Min. 10 G FOC connectivity
9. All the FOC connectivity mentioned above must be provided with a redundant pathway through a separate route. The above mentioned FOC connectivity may change or increase as per the requirement of the Client at the time of commissioning.
10. No Road cutting to be done for the laying of FOC, however, if required, it is to be done as minimum as possible for executing the work after approval from HSCC & AIIMS.
11. Ultrasonic Survey to be done before laying of FOC for the identification of existing services in Campus and feasibility of route to be identified. Report of Ultrasonic Survey is to be submitted before laying of FOC along with best suitable route for the laying of FOC.
12. Trenchless method to be followed for the laying of FOC. Identification Milestones to be placed along the path of the underground FOC at every 30 metres.
13. Supply, Installation, Configuration, Testing, Commissioning, Integration, Operation & maintenance of network solution for network components including the following:
   a. Core Switches
   b. Network Management Solution(NMS)
   c. Wireless Access points
   d. Wireless Controllers

   e. Firewalls/ UTMs
   f. Distribution Switches
   g. Access Switches
   h. Network Access Controller (NAC)
   i. Server Hardware

14. The bidder will arrange the power, UPS & Internet during the Installation, Configuration, and Testing period of the project.
15. HSCC will provide the space for keeping the materials during Installation, Configuration, and Testing.
16. All the necessary licenses for the above equipment to be provided as per the requirements.
17. All the above network equipment shall be offered with 5 years onsite comprehensive warranty and 24/7 support with response time within 4 hours & same day rectification (replacement of hardware).

The scope of work shall also include the following:

1. Design, configure, testing at works, packaging, transportation, supply, handling at site, installation, laying, erection, testing, integration, training, acceptance test, commissioning of communication networks, as applicable along with associated equipment, hardware, software on a turnkey basis, inclusive of 5 years comprehensive warranty for operation & maintenance.
2. Necessary cables including power cable and accessories as may be required for smooth and reliable operation of networking equipment.
3. The Bidder shall furnish complete details of acceptance tests proposed to be conducted before handing over the installation to the AIIMS, New Delhi.
4. Racks for mounting of network equipment including dressing of cables with proper marking on both sides in the rack.
5. All pipes & cable laying including termination, accessories including HDPE pipes, conduits/channels, supporting structures, clamps, identification tags, ferules etc. required for laying of cables.
6. All cable laying including Fibre Optics cables inside and outside the buildings including excavation work required for laying of cables, conduit etc. Laying and installation of the cable should be as per the standard of industry norms.
7. Supply of all spares required during erection, testing, commissioning and warrantee maintenance.
8. Minor civil works (if required) such as chipping/ cutting of floors for making grooves, making holes/ opening through walls, ceiling or floors, drilling of holes through steel structures and frames, grouting of frames, hooks on walls/ceiling etc. required for execution of work. After erection, surface shall be made good by plastering/painting to their original shape and finish.
9. Necessary Training & documentation including SoPs & Network Diagrams for IT staff of the AIIMS as per the requirements.
10. Bidder shall arrange for posting of required technical and other staff during erection, testing, commissioning, operation & maintenance of the systems.
11. Bidder shall arrange for posting of Project Manager onsite during project implementation.
12. Floor-wise network points are mentioned in the enclosed at Annexure-A. Approx. 14,000

Network points shall be required for LAN connectivity for the all the new blocks and NCI.

13. Site certification is to be done by the Bidder for Penta-scanning and certificate to be submitted for the performance warranty of 25 years.
14. OLTS test is to be done by the Bidder for FOC connectivity as per the requirement. (If any other test for ensuring the performance of CAT 6A and FOC cables is found to be mandatory at the time of installation, it should be done by the Bidder without additional cost.
15. Number of Indoor/outdoor wireless units shall be installed to cover all the area of the New Blocks at Both the Campus as per the requirements depending on the physical layout and capacity of the wireless units for establishing wireless connectivity.
16. Vendor should provide atleast “very good” signal quality consistently at all points in the premises. A heat map of whole premises should also be provided without any blackholes after conducting a site survey.
17. Any equipment, materials or supplies which may not be specifically mentioned, but are necessary for carrying out the contract work shall be in the scope of the Bidder and the system must be complete in all respects.

7.1.1.2 Additional specific terms of the contract for establishment of Wired and Wireless Network Solution.

1. All active components of the network shall be offered with 5 years comprehensive onsite OEM warranty.
2. Licensing – All the licenses of the software will be provided in the name of the client (AIIMS, New Delhi).
3. Bidder shall be solely responsible for all the operations & maintenance of all the items supplied and installed for the period of 5 years from the date of commissioning and handing over of all the items to Client.
4. After award of work and at the time of implementation, in case the quoted model(s) are out- dated and new upgraded model introduced in the market, then Bidder shall supply the latest upgraded model without any extra charges. All the latest product and technology to be used at the time of establishment of the LAN and Wi-Fi System at site. Any product and technology should not be obsolete or end-of-life by current standards.
5. If any promotional scheme is launched by the manufacturer at the time of supply of the item, all the benefits of the scheme will be given to the client.
6. Bidder has to provide the plan, design and site preparation as per requirement and as directed to the satisfaction of AIIMS & HSCC and as per terms of the technical specifications.
7. Detailed shop drawings, concept drawings, indicating line diagram, route diagram showing details of laying underground, overhead or under wall cables, showing details of cable, switches, joint etc. complete in all respects to be submitted to AIIMS & HSCC for approval before ordering any item & start of execution work within 21 days of award of work. The design if required will be revised as per direction of AIIMS & HSCC before approval.
8. Before ordering and laying cables, drawings and diagrams etc will be vetted from electrical, fire, civil, air-conditioning departments of AIIMS, and HSCC.

9. Bidder is responsible for all unpacking, assembling, wiring, installation, cabling between equipment and components and connection to power supplies. They will test all Systems operations and perform all the necessary setup, configuration and customization for successful operation of the Network at site.
10. The Network Solution will be accepted only when authorized persons from the AIIMS & HSCC have given satisfactory performance report of the installation.
11. LAN & Wi-Fi will be used for running Hospital Management Information System, PACS (Picture Archival and Communication System), internet and network facility, Access control system for employees, , Biometric Attendance System, Patient Access System through scanning, display system including outside OPD / Consultant rooms, Common rooms Hall etc., Public Address System, Internal Telemedicine (Video Conferencing), Queue Management System, traffic and parking management etc.& other applications as per the requirement of the AIIMS, New Delhi.
12. The entire infrastructure to be developed for providing above solutions and services with adequate speed and security as per the requirement.
13. Inspection – The inspection shall be carried out by authorized representative of HSCC and AIIMS New Delhi. AIIMS New Delhi (client/purchaser) has the right to inspect and/or to test the material to verify its conformity with the contract and in case any inspected/tested good(s) fail to perform to the specifications, the client may reject them and the Bidder shall either replace the rejected goods or make alteration necessary to meet the specifications free of cost to the Client/purchaser. The Client also reserves the right to involve any third party assessor to test and/or verify the same.
14. Bidder should provide the standard technical literature (not photocopies) of the entire offered product.
15. LAN should be at least 100G Inter Core Switch, 40 Gigabit Ethernet on Optical fiber backbone from Core Switch to Distribution Switches and 10 Gigabit from Distribution Switches to Access Switches, and 1G from Access Switches to nodes. Bidder may propose a higher performance system which is capable to handle the needs of all new blocks AIIMS and NCI, Jhajjar.
16. The Bidder shall supply all the installation material/ accessories/ consumables (e.g. screws, clamps, fasteners, ties anchors, supports, grounding strips, wires, fiber connection kits etc.) necessary for the installation of the systems.
17. The Bidder shall be responsible for providing proper "Electrical ground" at all the required points as per the approved IEEE standards for Grounding of Sensitive Electronic Equipment and as per the OEM/industry guidelines.
18. The Bidder shall install and wire the UPS power at required locations and provide proper electrical ground for the same before installation of the equipment. Civil works if any required for installation of the system will be the responsibility of the Bidder.
19. All the work shall be done in a conscientious manner as per the OEM guidelines and best industry practices. The system shall be subjected to inspection at various stages. The Bidder shall follow all Safety Regulations and practices.
20. The Bidder shall configure quality of service parameters on network switching devices for end-to-end QoS for critical traffic over the network.
21. Bidder shall be responsible for integration of security components in the network to ensure a secured network access for users.

22. Bidder shall configure network management policies for managing all the network and security devices using network management systems.
23. Bidder shall prepare detailed acceptance testing plan (ATP) for each of the components i.e. Network (LAN & Wi-Fi system) and submit the same to AIIMS, New Delhi.
24. All the functionality, features and configuration shall be documented for all the equipment/components and shall be demonstrated with respect to the documentation prepared.
25. The Bidder shall be responsible for obtaining approvals (if any) for any Statutory &Regulatory requirements from any of the authorities.
26. Bidder shall use his own sets of tools, tackles, etc. required for erection, testing, commissioning and warrantee maintenance of the system.
27. Compliance for all the Network components (LAN & Wi-Fi) to be submitted along with technical bid as per the format enclosed at Annexure–D.
28. Network up time should be continuous throughout the warranty period covering 24x7 without fail and as per the requirement of the institute.

7.1.1.3 Other terms & conditions and requirements

1. The network solution including hardware & system software set up should be able to integrate with various software and system already running at AIIMS, New Delhi.
2. The system should be capable of handling the HMIS, PACS and other applications as per the requirement of the Client.
3. The network set up should be capable of providing high bandwidth internet/network connectivity in all the desktops, laptops, tablets or any other device as per the requirement.
4. The Wi-Fi should be capable of connecting all the devices i.e. desktops, laptops, tablets etc. and offer high bandwidth connectivity.
5. The system should be capable of deploying all the policies (i.e. Network, Security, etc.) as per the requirement of AIIMS, New Delhi.
6. The Bidder shall bear for any damage occurring during supply, installation, testing, commissioning & activation of network components, computer hardware etc. The same has to be rectified by Bidder at their own cost. In case Bidder fails to do rectification, the same shall be rectified by HSCC/client and involved cost will be recovered from the Bidder.
7. In case of additional hardware, software or any other work is required for completeness of the system, the same shall be provided by Bidder without any extra charges.

7.1.1.4 Guarantee/Warranty and Comprehensive Operations & Maintenance

1. The Bidder shall warrant that the Goods supplied under the Contract are new, non-refurbished, unused and recently manufactured; shall not be nearing end of sale / end of support; and shall be supported by the Bidder along with service and spares to ensure its efficient and effective operation for the entire duration of the contract. The manufacturer should also submit guarantee/warranty that it will keep the AIIMS, New Delhi informed of any up-date of the equipment over a period of 5 (five) years from the date of acceptance.
2. The Bidder should ensure that the manufacturer will supply regularly any items or spare parts for satisfactory operation of the equipment during the period of Guarantee/warranty

and Operation & maintenance period.

3. The Bidder hereby guarantee/warranty that the goods/stores/ articles supplied to the AIIMS under this contract shall be of the best quality and workmanship, strictly in accordance with the specifications and standards contained/mentioned in the tender and shall operate properly and safely. All recent design improvements in goods, unless provided otherwise in the Contract, shall also be made available. The HSCC/AIIMS will be entitled to reject the said goods/stores/ articles or such portion thereof as may be discovered not to conform to the said description and quality. The Bidder shall, if called upon to do so, replace goods/stores/articles within a period of fourteen days the goods/stores/ articles or such portion thereof as rejected by the HSCC or AIIMS. In such an event, the penalty will be imposed as per penalty clause. On such rejection, goods/stores/articles will be at the Bidder's risks and all the provisions herein contained relating to rejection of goods, etc. shall apply. Otherwise the Bidder shall pay to the AIIMS such damages as may arise by reason of breach of the conditions herein contained.

4. Bidder should categorically confirm that they will give "After sales services" during guarantee/ warranty period from the date of installation, satisfactory commissioning, acceptance and handing over of the respective phase of project. The firm must ensure that they will provide every calendar year, at least 4 number of preventive maintenance to all of the equipment and also any number of emergency visits during each year of Warranty/Guarantee and operation & maintenance period. Preventive maintenance has to be done in consultation with AIIMS, New Delhi team.
5. During the guarantee/warranty period and Operation & maintenance period the firm will be required to maintain the Hardware, Local Area Networking, Security Solution and other equipment/product supplied under this tender in good working condition so as to ensure fault free operation of the system for 24 hours on all the days of the year including holidays and Sundays.
6. During the guarantee/ warranty period, the Bidder shall cover costs of all the items and spares.
7. Bidder shall be responsible for the supply, installation, testing, commissioning & activation of all network components.
8. The payment shall be made as per the payment terms and conditions mentioned in the tender document.

7.1.2 Establishment of Server rooms, Data Centre (DC) and Disaster Recovery Centre (DRC)

All the related works to make Server Room operational covered under the scope of work i.e.:

1. Elevated Flooring with in-floor channels for cabling, drainage, and services
2. Precision Redundant Air-conditioning
3. Cabling (Network Connectivity)
4. Electrical Work
5. Redundant power supply & redundant UPS
6. UPS installation with adequate cooling
7. Biometric Access Control
8. Plumbing for drainage

9. Well insulated and dust proof server room with double glazing & fire safety etc.
10. Any other related work for the completeness of the work.

Bidder is required to execute all above work as per the requirement to make the Server room functional. Cost is to be included in the tender.

7.1.3 Providing Manpower for Operations and Maintenance and Helpdesk

7.1.3.1 Operations, Maintenance & Support Services

The Bidder shall be fully responsible for the entire LAN & Wi-Fi System and connectivity from Computer Facility & NOC2 and provide onsite comprehensive (manpower and parts) operation & maintenance support to maintain the same. The scope of work includes:

1. The Bidder, shall be fully responsible for the entire LAN & Wi-Fi System and provide onsite comprehensive (manpower and parts) operation & maintenance support to maintain the same for the above-mentioned period of support.
2. Day to day Onsite Comprehensive Operation & Maintenance Services support including labour shall be provided for all IT components i.e. Hardware, Software, Servers, Networking equipment, cabling etc. supplied as part of the IT & Network Solution.
3. The Bidder shall provide 24x7 onsite technical support as per below
    a. Both Campuses: 1 network administrator per campus
    b. Both Campuses: 1 network engineer per 1000 nodes per shift
    c. New Delhi Campus: 1 support staff per block per shift; Jhajjar Campus: 2 support staff per shift
4. Their shift timings may be redistributed as per the requirement of the client AIIMS New Delhi.
5. Their deployment ratios may be decreased as per the requirement of the client AIIMS New Delhi.
6. Period of support: The IT Network solution will enter Operations & Maintenance Support Services phase from the date of commissioning of the services. It may be noted that the commissioning of services in various blocks of AIIMS and NCI Jhajjar will be staggered and will vary as per the date of commissioning of the network solution at various blocks/locations. The period of Operations & Maintenance Support of the tender will be ten years (5 years warranty period + 5 years CAMC period), starting from the date of commissioning of network solution in the BLOCK/BUILDING. It should be noted that it does not include any technical manpower posted at the location before the date of commissioning of the Network Solution in those blocks/locations.
7. Type of Support: 24x7 onsite support both for AIIMS Campus and for the NCI Jhajjar campus.
8. Addressing and fixing any major or minor technical snags, technical problems or technical issues reported by the end user in the installed network solution.
9. Attending the breakdown call and make all efforts to rectify faults related to failure of hardware/network at site with minimum possible time and maximum up to 24 hours from the time of reporting of fault.
10. Make further customizations / any changes in the network solution as the need may arise from time to time during the above said period, without any extra financial cost.
11. Co-ordinate with the authorized person of the AIIMS, New Delhi at site for resolution of

all technical issues, snags and configuration changes required.

12. A request for hardware operation & maintenance shall be recorded as service request, which includes requests such as installation, re-installation, change of network configurations etc. Expected turn-around time for such service request is within 6 hours of logging the service request. Suitable alternative arrangements to be provided in case of delay.
13. Operation & maintenance support should be provided as per the standard practices and as per the specification and manual of the equipment, complete in all respect and to the satisfaction of the client.
14. Installation of firmware, software or patches for all networking devices (Firewall, NMS, Wireless Access Points, Wireless controller etc.) as needed to be upgraded time to time will be done.
15. Licenses and up-gradation of the OS.
16. Preventive maintenance of the hardware and its related softwares etc.
17. The vendor shall ensure that the payment to the manpower deployed is in accordance with or above the minimum wages proposed by the central government at all times. The vendor shall also adhere to all provision of the Contract Labour Act and all applicable laws.
18. Help Desk Services: The Bidder has to maintain Dedicated on site 24x 7 Help Desk Service for end users manned by support personnel as mentioned above, to attend and initiate action on the problems related to IT network solution and services setup under the scope of this contract.
    a. Help desk services should act as a single point of contact, to solve day-to-day problems of end users.
    b. The help desk should be capable of initiating the solution to the problem through network engineers and network administrators.
19. The Bidder would prepare an escalation matrix in consultation with the IT team of the AIIMS for the different categories of calls.
20. Help Desk's responsibility is to generate certain reports to track following:
    a. Call Analysis
    b. Call Trend
    c. Call History Report
    d. Daily call completed and pending Reports along with reason for not completion
    e. Other reports desired by AIIMS
21. The deliverables and the activities of the helpdesk service, related to IT network solution and services of New OPD Block, would also include the following.
    a. Log user calls and give them a call ID/ Ticket number
    b. Assign severity level to each call
    c. Track each call to resolution iv. Escalate the call to the relevant team like User support, System Administration, Network administration, OPD application support etc. which is capable of resolving the issue and keep the IT team of the AIIMS, New Delhi informed suitably.
    d. Analyze the call statistics.
22. The selected Bidder will have to arrange its own hardware and software tools, if any needed, to run the help desk facilities as agreed by AIIMS IT team.
23. The help desk service shall also include the generation of trouble tickets and submitting

unresolved problems to the appropriate internal service providers.

24. All the related work to make help desk operational covered under the scope of work i.e.:
    a. Cabling (Networking)
    b. Electrical work
    c. Connection with UPS
    d. Furniture as per the requirement
    e. Supply, installation, customization, testing, implementation, training and maintenance of help desk software.
    f. Any other work for completion of the work as per the requirements.
25. Bidder is required to execute all above work as per the requirements to make the help desk functional. Cost is to be included in the tender.
26. Following is the minimum qualification and experience required for the on-site deployment of manpower for operations & maintenance support

Sr. No.	Manpower (number deployed as per norms cited above)
1	**Network Administrator:** Qualification BE/B.Tech in relevant area/MCA OR equivalent; with minimum 5 years Post Qualification experience in relevant area (Networking and Data Centre).
2	**Network engineers:** Qualification BE/B.Tech in relevant area OR equivalent; with Minimum 2 years Post Qualification experience in relevant area
3	**Support personnel:** Graduate with good knowledge of Hindi & English and well versed with Computer Environment/operations, good typing skills and having minimum 1 year experience.

Minimum requirement of manpower for Part B: Comprehensive Operation, Maintenance and support services during warranty period - for 1-5 years (Actual requirement may vary)

Sr. No.	Description	Quantity for New OPD Block (Approx. 3000 nodes)	Quantity for Mother and Child Block (Approx. 2000 nodes)	Quantity for Surgical Specialties Block (Approx. 800 nodes)	Quantity for NCI Jhajjar (Approx. 8000 nodes)	Total
1	Network administration Services	1			1	2
2	Network engineering services (One network engineer per 1000 nodes per shift)	9	6	3	24	42

3	Network helpdesk services (For AIIMS campus One support staff per block per shift) (For NCI campus 2 support staff per shift)	3	3	3	6	15

Any other specialist is required for maintaining IT infrastructure the same shall be covered in the current scope. No additional charges paid for the extra manpower.

7.1.3.2 Other terms & Conditions for operation & maintenance support services

1. A lease line for network connection of all the blocks will be provided by AIIMS, New Delhi.
2. During the Operation & maintenance period, if Bidder fails to deliver the services required for operation & maintenance at any point of time, the same shall be done through other Bidder without giving any notice to the originally selected Bidder and the cost involved will be recovered from the originally selected Bidder as risk purchase.
3. Performance Bank Guarantee for the operation & maintenance should be made in favour of Director, AIIMS, New Delhi. A separate PBG will be taken for the post-warranty period equivalent to 10% of the total CAMC cost (6th to 10th year) and will be released after the contract period by the client as per the terms & conditions.
4. Attendance of manpower engaged for operation & maintenance shall be verified by AIIMS and their payments to be made by client as per the payment terms.
5. Agreement for operation & maintenance services will be made between client & Bidder.
6. HSCC and AIIMS, New Delhi shall involve in the selection process of all candidates. Resume consisting of their experience &qualifications should be submitted to HSCC& client. HSCC &client reserves the right to deploy or reject the selected candidates/engineers for the operation & maintenance.
7. The Bidder must pay minimum wages to the engineers as per existing laws at par with industry norms. Candidates to be selected by the selection committee and after approval from HSCC/client.

7.1.4 Special Terms and conditions for development of IT solution and services

1. AIIMS, New Delhi will have the option to install the solution and obtain services in a phased manner if required.
2. Deliver training services for the AIIMS staff for knowledge transfer both on the functional and technical aspects.
3. Provision of on-going operation & maintenance and support, including software and firmware upgrades.
4. Resolution of technical issues and/ or problems.
5. Installation of Hardware, including–
    a. Appropriate Server(s) along with OS, associated database & other related software for System security, including firewall, Controller, NMS, NAC, UTM etc.
    b. Associated hardware for Business Continuity & Backup.
6. Adequate stock (minimum 10% of the installed) of active & passive networking components including switches, cables, patch cords etc., to ensure immediate replacement

in case of failures.

7. Providing post-implementation Operation & maintenance Support for all components listed above.
8. The Bidder is expected to provide complete specifications of all the products and services quoted for, together with the details of the manufacturer. The AIIMS, New Delhi reserves the right to make appropriate verifications on all the products / components.
9. **Supervisory Committee Formation**: A supervisory committee shall be constituted which will review the progress and provide necessary advice for mid-course corrections to the service provider. The committee will comprise of representatives of the AIIMS, New Delhi and/or HSCC.
10. **Documentation:** It is the responsibility of Bidder to provide at least the following documents to AIIMS, New Delhi:
    a. User Manuals
    b. Training Manuals
    c. Implementation Manuals
    d. All licenses
    e. All configuration details
    f. Specification of all items supplied

7.1.4.1 Service Level Requirements from the IT solution and services

7.1.4.2 Guaranteed Uptime & Calculation of Uptime

Operation & maintenance support shall ensure a guaranteed uptime of not less than 99.8%. The Bidder will provide a monthly uptime report, calculated as follows, to AIIMS, New Delhi:

On all 24 hrs x 365 days a year, the network shall be up and running. It is assumed that New OPD block will be working, 24 hrs round the clock for 365 days in a year and hence the total up time works out to 365 x 24= 8760 hour/annum. 0.2% downtime accordingly shall mean 17.5 hours in a year. However, the network shall be maintained in such a manner that on no occasion the network shall be down for more than 1 hour at a stretch and 10 hours in a calendar month. The same shall be construed as failure of operation & maintenance support to rectify the system within the stipulated period and the penalty as indicated below shall be recovered, even though the total down time in the year up to that point of time/month/year may be less than the permissible downtime. If 5% of switches or 5% of cablings faulty, it will be assumed as downtime.

7.1.4.3 Downtime Penalty

For network downtime as defined above beyond the permissible period in a day/month/year, a penalty at the rate of Rs.5000/- per hour will be recovered for every hour of failure. However, if only a portion of the network or sub-network is down beyond the permissible limits, a penalty of Rs.1000/- per hour will be levied. The penalty time shall be arrived on the basis of 24 hours operation on each working day. The penalty will be deducted from bills/ performance security.

Violation on more than three occasions shall make the vendor liable for debarring / backlisting with forfeiture of the PBG.

7.1.4.4 Penalty on the account of Operations & Maintenance Support Services

Service	Target	Penalty for NOT meeting target
Operations, maintenance Support Services	Resolution of all minor issues within 2 hours	Rs.500/-per call with delayed resolution of the issue
	Resolution of all major issues within same day	Rs.1000/-per call per day of delay

Violation on more than three occasions shall make the vendor liable for debarring / backlisting with forfeiture of the PBG.

7.1.4.5 Penalty on the account of violation of Labour Laws

In case of violation of any of the labor laws or guidelines for minimum wages, a penalty of Rs 5000 per episode per person shall be levied. Violation on more than three occasions shall make the vendor liable for debarring / backlisting with forfeiture of the PBG.

7.1.4.6 Penalty on the account of Delay in Commissioning

The entire work, shall be completed and ‘Go Live’ within 4 months from the date of hand over of the site/commencement letter.

Failing this, liquidated damages at a rate of 1/2 % of the work order amount per week of delay beyond the stipulated period for the delayed portion of the contract will be levied for delay.

7.1.5 Definitions & Reference

1. Server-class systems Service Level requirements shall provide for services to ensure availability of appropriate server platform (e.g. type & no. of processors, network card, memory, etc.) coupled with operating system and middleware, for each specified server type. The services shall also include installation of application as required. These services shall be available to the AIIMS, New Delhi and NCI Jhajjar on an ongoing basis.
2. Security service: The Bidder shall be responsible for development, documentation and implementation of Network security management systems.
3. The performance of the Bidder will be monitored and recorded as necessary over the duration of the contract with respect to satisfactory fulfillment of all contractual obligations. Performance assessments may comprise of:
    a. Delivery of services
    b. Condition of delivered equipment
    c. Compliance with service levels
    d. Availability of services within established timelines
4. The Bidder shall assemble and create regular reports on the performance of application functions, in order to assist in the effective management of the Service agreement, and enable continuous improvement of the in-scope services that the AIIMS, New Delhi receives.
5. Routine meetings and reporting processes must be defined to ensure a smooth interface and timely resolution of issues. The Bidder must provide a single interface to coordinate the delivery of all services.

7.1.6 Project and Technical Risk Management Plan and Procedures

The Bidder will be responsible for assisting the AIIMS, New Delhi in Identifying and assessing potential technical risks of the project as well as identifying and managing actions to avoid, mitigate, or manage those risks. Bidder is responsible for providing appropriate methods, tools and techniques for active identification and assessment of project technical risk; development of risk avoidance, mitigation, or management strategies; and monitoring and reporting of risk status throughout the life of the project, the AIIMS, New Delhi shall fully co-operate with the Bidder in this regard.

7.1.7 Timeline

The entire work, shall be completed and 'Go Live' within 4 months from the date of commencement letter for that block (s).

Failing this, liquidated damages as specified previously will be levied. The successful Bidder shall submit a Bar Chart / Programme for completion of supply, erection & commissioning of the various components & sub- assemblies along with manpower schedule.

7.2 Ownership of Data

1. The Bidder shall be the custodian of such data, and shall also ensure its security and integrity.
2. The Bidder shall ensure the provision of appropriate and adequate security levels, for protection of such data and other technology resources, which shall come into its custody during the implementation of the proposed solution.
3. The infrastructure for the proposed solution, at each of the sites, shall be strictly and exclusively used by the Bidder for processing data related to the all blocks and NCI, Jhajjar. Under no circumstances shall the infrastructure be used for any other purpose by the Bidder.
4. The AIIMS, New Delhi / its authorized representative(s) shall conduct periodic / surprise security reviews and audits, to ensure the compliance by the Bidder to these control / access provisions.
5. The Bidder shall develop and implement an "IT Security Policy" for the proposed IT solution. This IT Security Policy shall be in line with National and International guidelines &standards. The Bidder shall also keep itself updated with the latest IT Security Policy of the Government.
6. All the latest hardware and software should be provided with latest Technology, maximum up to six months old. Beyond that it will not be acceptable.
7. Cost of the any additional hardware and software to be required for completeness of the system as per the Client's requirement to be covered in the present scope and Bill of Quantity. No additional charges to be paid for extra item.
8. All the licenses of the software will be provided in the name of the client (AIIMS, New Delhi).
9. All the server Hardware shall be provided from day 1 as per the specification mentioned.

7.3 Approval of Materials

Technology (Hardware and Software) used on the Works shall be latest, new and of the best quality available, confirming to the relevant specifications and as per good Engineering practice. Prior approval shall be obtained in writing from the Client for all materials proposed and when necessary approved sample duly identified and labeled shall be deposited with the officers of AIIMS and shall be kept at site. “List of approved makes” indicates make/manufacturer generally acceptable but final choice of make/manufacturer of material & models shall be with the client.

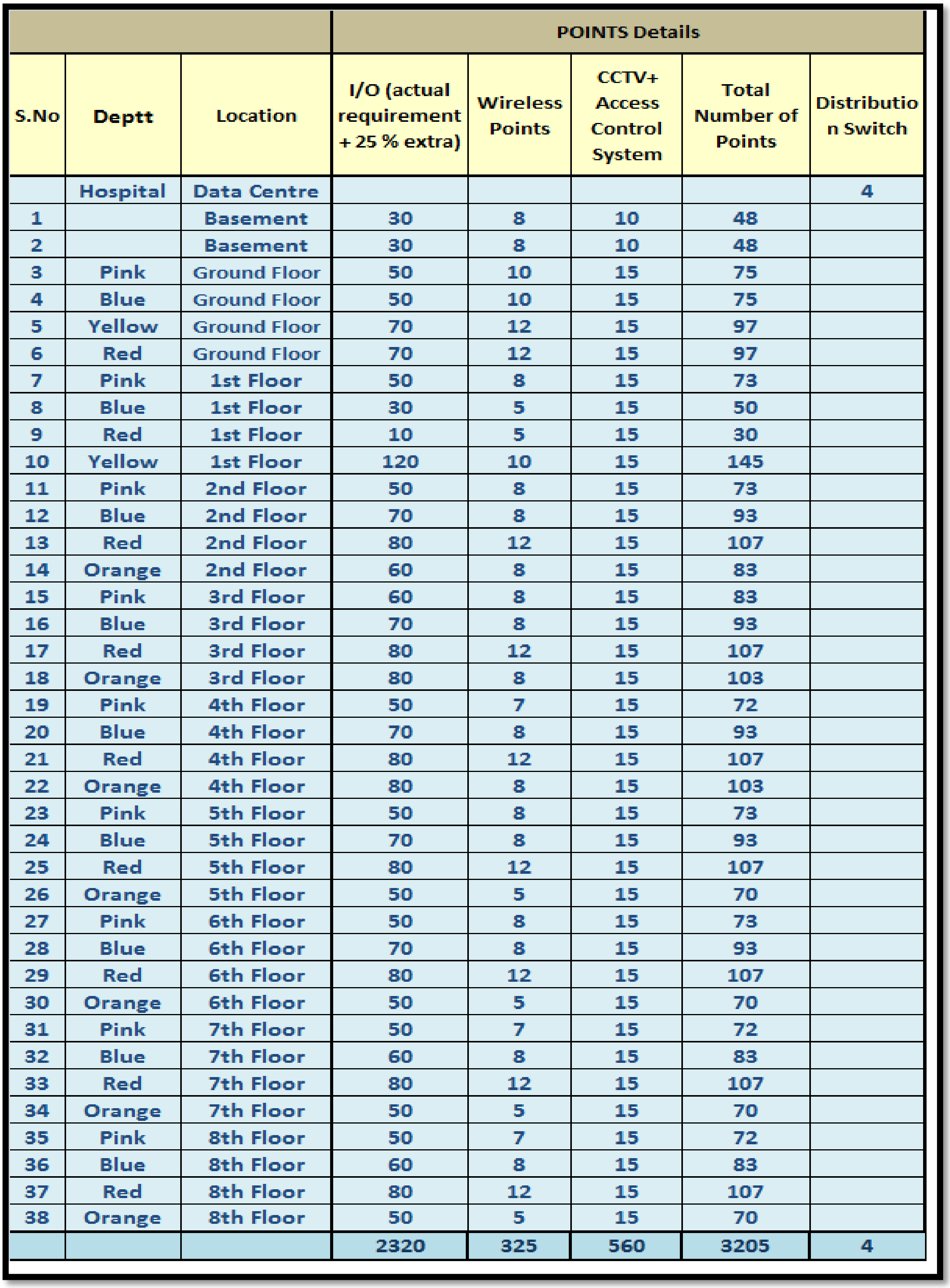
7.4 List of Annexure of Volume-IV

Sr. No.	Name of Annexure	Description
1	Annexure-A	Distribution of Active and Passive items – Block-wise and Details of Network Points
2	Annexure-B	Proposed Network diagram
3	Annexure-C	Technical Specification for Active and Passive items of LAN and Wi-Fi
4	Annexure-D	Technical Compliances of Active & Passive Devices

Annexure-A

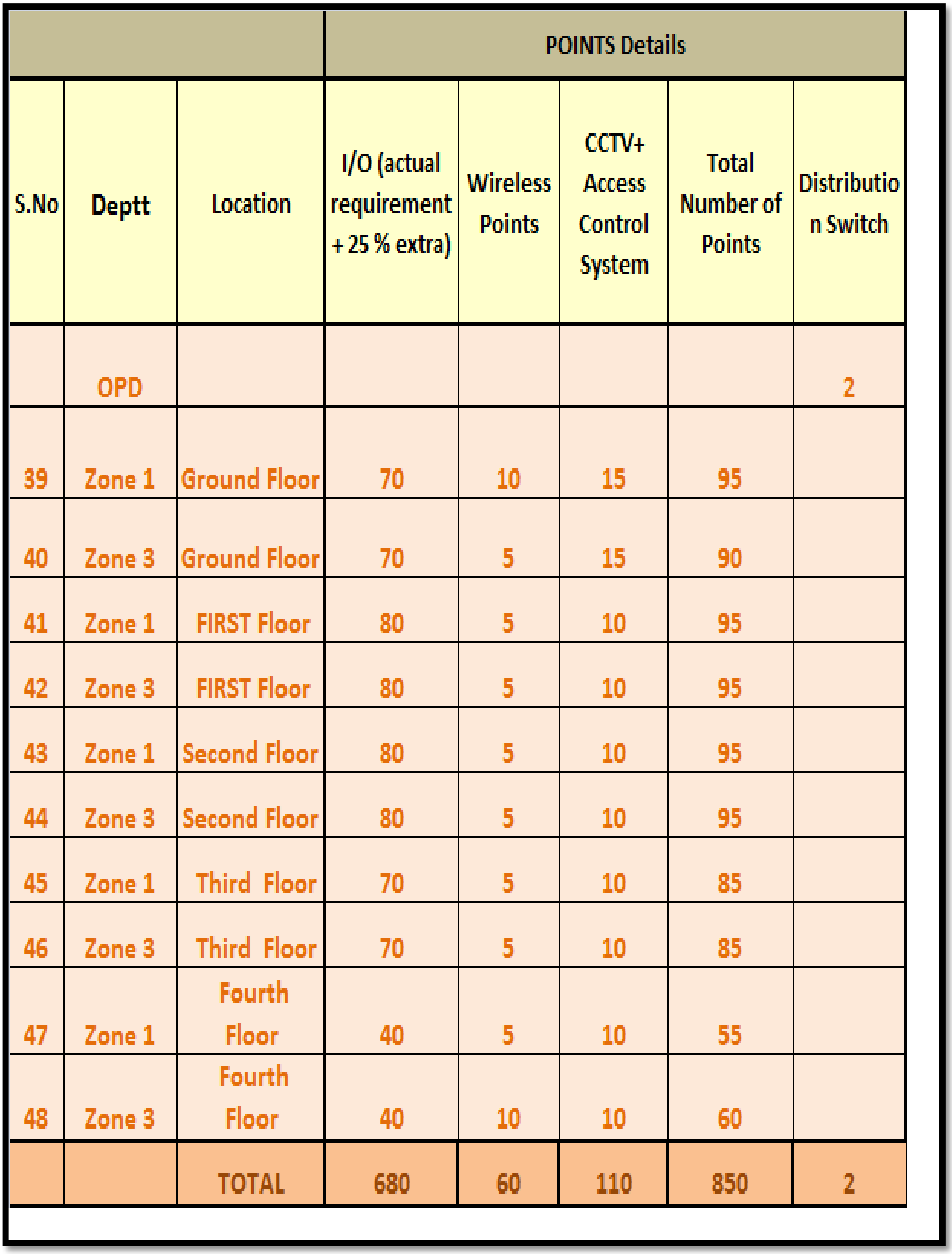
7.5 Distribution of Active and Passive items – Block wise (NCI Jhajjar Campus)

7.5.1 Hospital Block



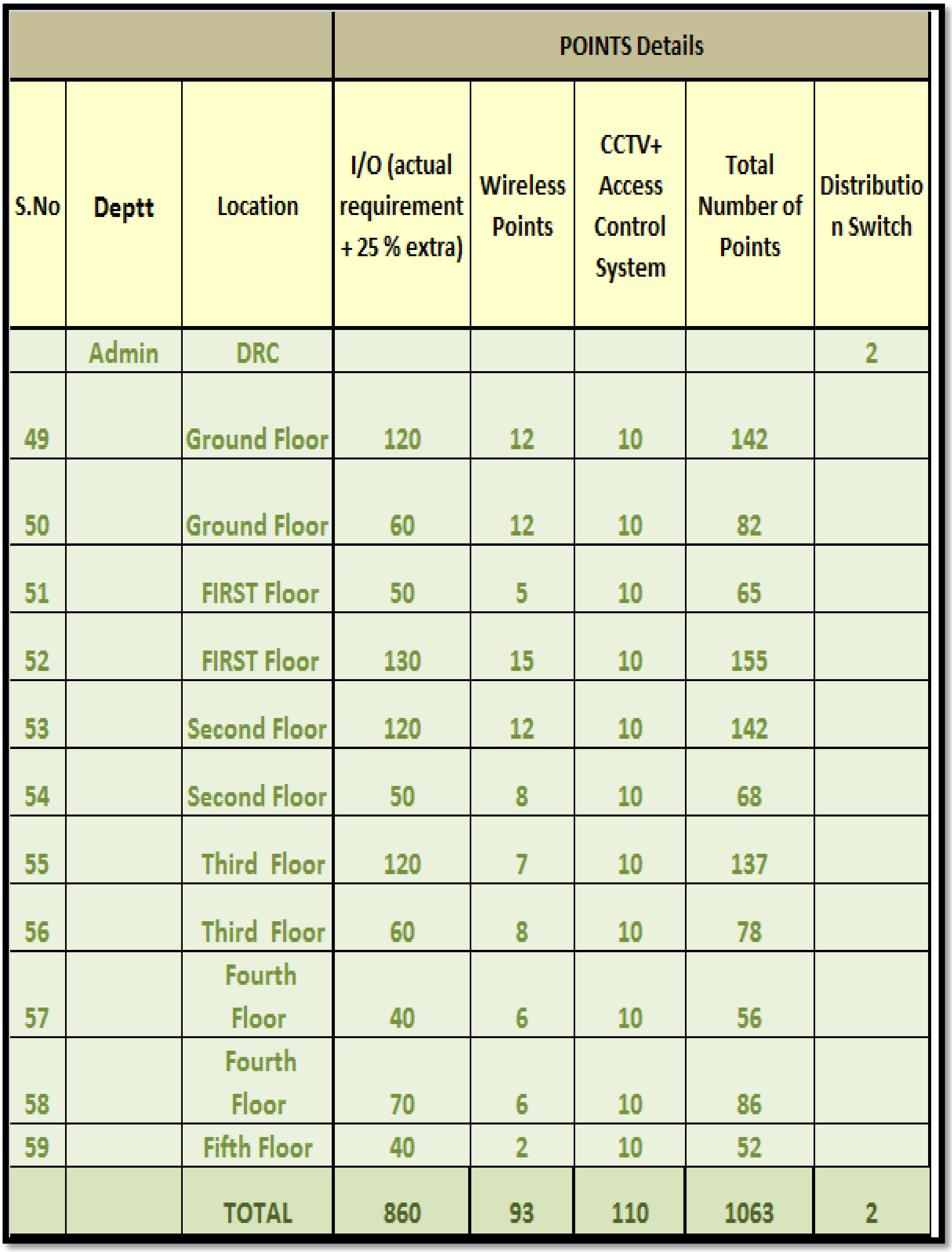
			POINTS Details				
S.No	Deptt	Location	I/O (actual requirement + 25 % extra)	Wireless Points	CCTV+ Access Control System	Total Number of Points	Distribution Switch
	Hospital	Data Centre					4
1		Basement	30	8	10	48	
2		Basement	30	8	10	48	
3	Pink	Ground Floor	50	10	15	75	
4	Blue	Ground Floor	50	10	15	75	
5	Yellow	Ground Floor	70	12	15	97	
6	Red	Ground Floor	70	12	15	97	
7	Pink	1st Floor	50	8	15	73	
8	Blue	1st Floor	30	5	15	50	
9	Red	1st Floor	10	5	15	30	
10	Yellow	1st Floor	120	10	15	145	
11	Pink	2nd Floor	50	8	15	73	
12	Blue	2nd Floor	70	8	15	93	
13	Red	2nd Floor	80	12	15	107	
14	Orange	2nd Floor	60	8	15	83	
15	Pink	3rd Floor	60	8	15	83	
16	Blue	3rd Floor	70	8	15	93	
17	Red	3rd Floor	80	12	15	107	
18	Orange	3rd Floor	80	8	15	103	
19	Pink	4th Floor	50	7	15	72	
20	Blue	4th Floor	70	8	15	93	
21	Red	4th Floor	80	12	15	107	
22	Orange	4th Floor	80	8	15	103	
23	Pink	5th Floor	50	8	15	73	
24	Blue	5th Floor	70	8	15	93	
25	Red	5th Floor	80	12	15	107	
26	Orange	5th Floor	50	5	15	70	
27	Pink	6th Floor	50	8	15	73	
28	Blue	6th Floor	70	8	15	93	
29	Red	6th Floor	80	12	15	107	
30	Orange	6th Floor	50	5	15	70	
31	Pink	7th Floor	50	7	15	72	
32	Blue	7th Floor	60	8	15	83	
33	Red	7th Floor	80	12	15	107	
34	Orange	7th Floor	50	5	15	70	
35	Pink	8th Floor	50	7	15	72	
36	Blue	8th Floor	60	8	15	83	
37	Red	8th Floor	80	12	15	107	
38	Orange	8th Floor	50	5	15	70	
			2320	325	560	3205	4

7.5.2 OPD Block



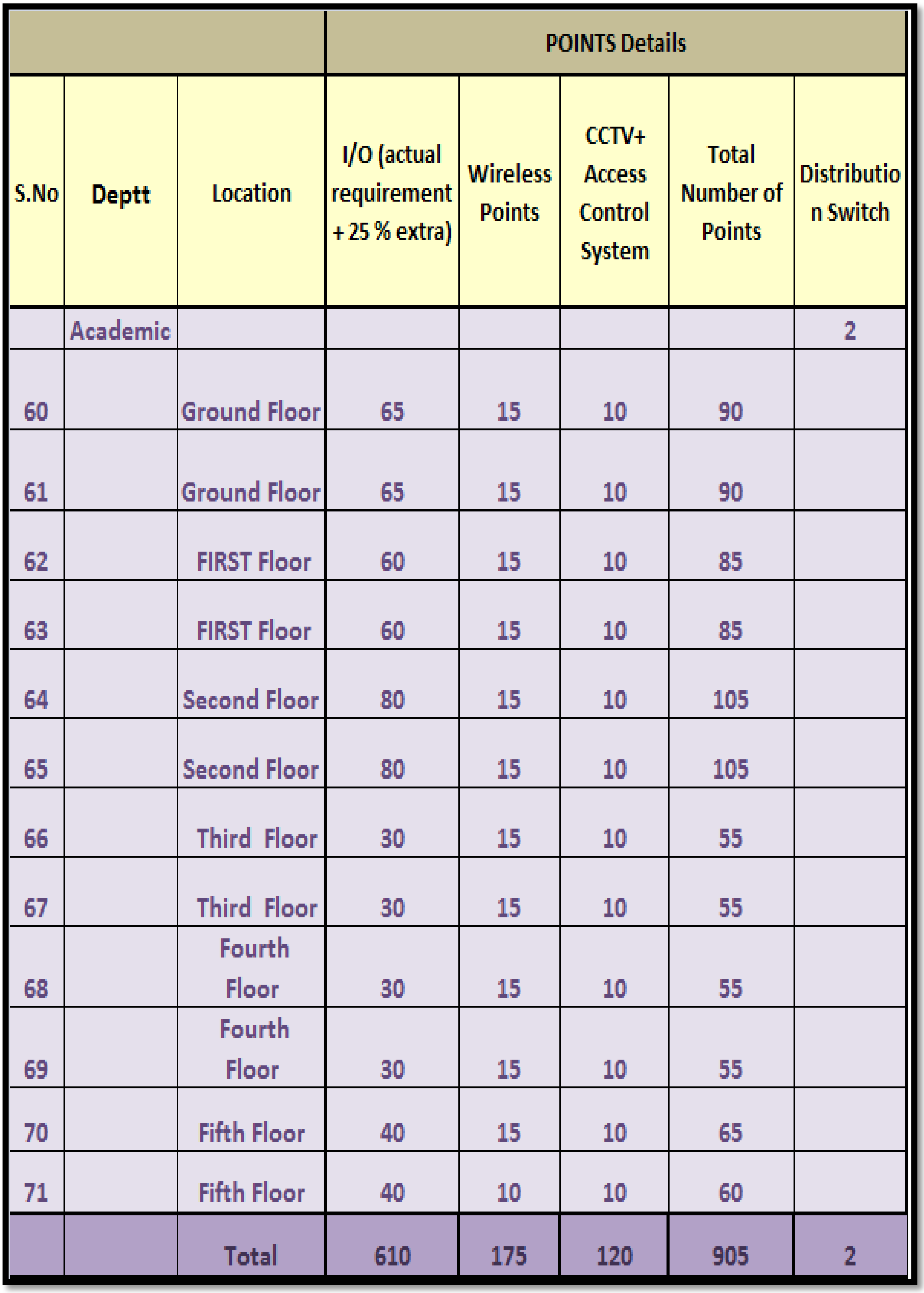
			POINTS Details				
S.No	Deptt	Location	I/O (actual requirement + 25 % extra)	Wireless Points	CCTV+ Access Control System	Total Number of Points	Distribution Switch
	OPD						2
39	Zone 1	Ground Floor	70	10	15	95	
40	Zone 3	Ground Floor	70	5	15	90	
41	Zone 1	FIRST Floor	80	5	10	95	
42	Zone 3	FIRST Floor	80	5	10	95	
43	Zone 1	Second Floor	80	5	10	95	
44	Zone 3	Second Floor	80	5	10	95	
45	Zone 1	Third Floor	70	5	10	85	
46	Zone 3	Third Floor	70	5	10	85	
47	Zone 1	Fourth Floor	40	5	10	55	
48	Zone 3	Fourth Floor	40	10	10	60	
		TOTAL	680	60	110	850	2

7.5.3 Administrative Block



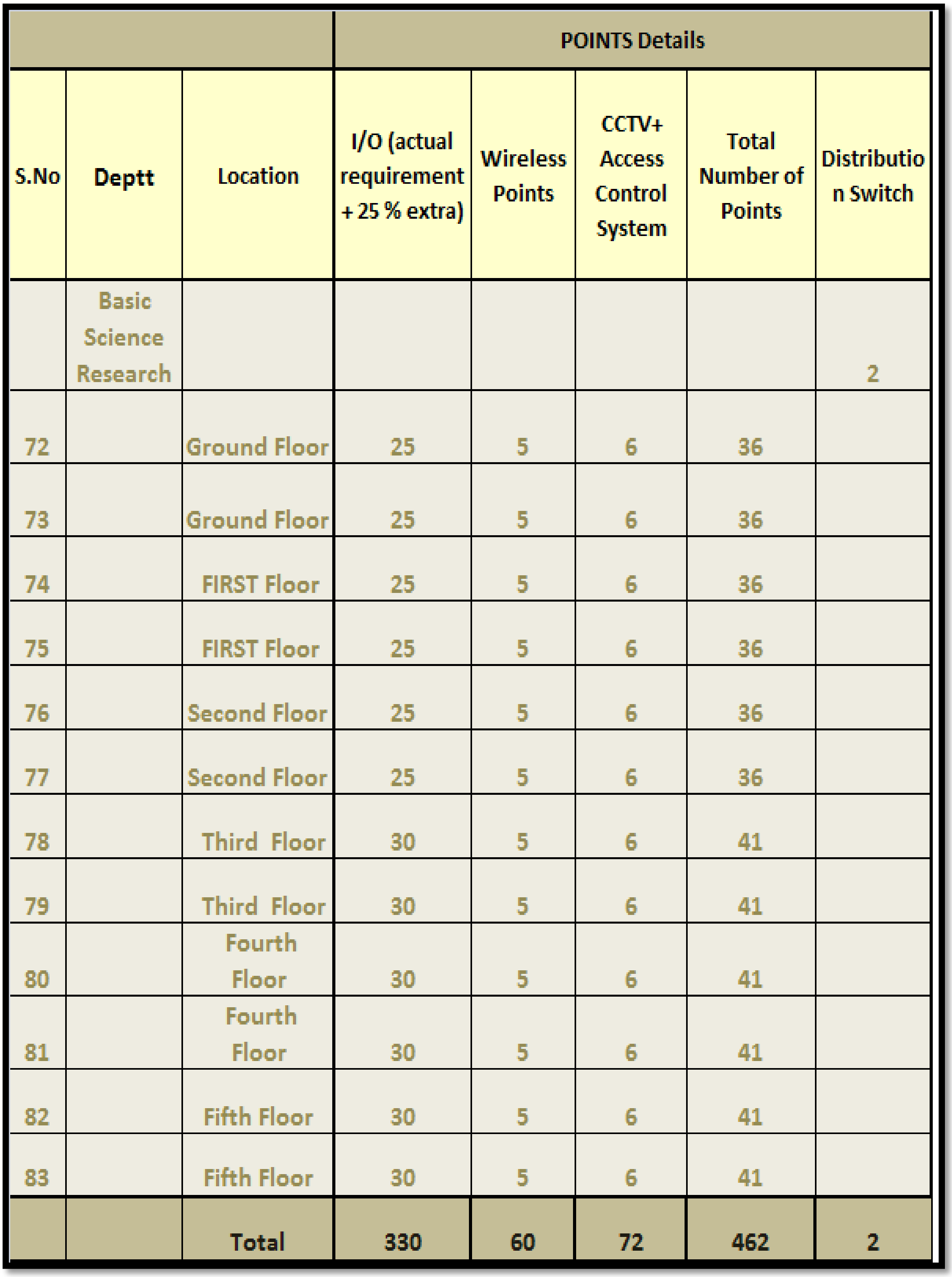
			POINTS Details				
S.No	Deptt	Location	I/O (actual requirement + 25 % extra)	Wireless Points	CCTV+ Access Control System	Total Number of Points	Distribution Switch
	Admin	DRC					2
49		Ground Floor	120	12	10	142	
50		Ground Floor	60	12	10	82	
51		FIRST Floor	50	5	10	65	
52		FIRST Floor	130	15	10	155	
53		Second Floor	120	12	10	142	
54		Second Floor	50	8	10	68	
55		Third Floor	120	7	10	137	
56		Third Floor	60	8	10	78	
57		Fourth Floor	40	6	10	56	
58		Fourth Floor	70	6	10	86	
59		Fifth Floor	40	2	10	52	
		TOTAL	860	93	110	1063	2

7.5.4 Academic Block



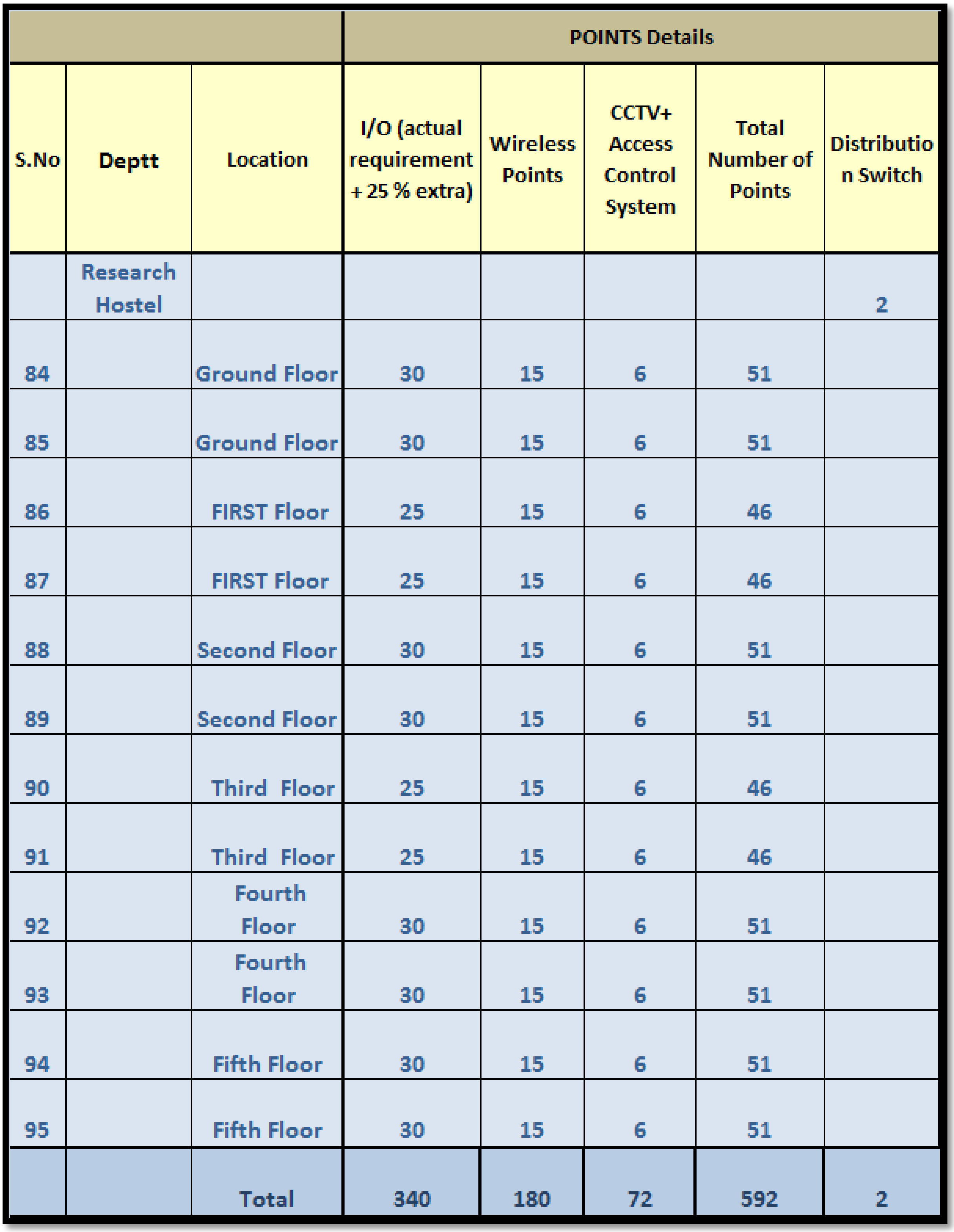
			POINTS Details				
S.No	Deptt	Location	I/O (actual requirement + 25 % extra)	Wireless Points	CCTV+ Access Control System	Total Number of Points	Distribution Switch
	Academic						2
60		Ground Floor	65	15	10	90	
61		Ground Floor	65	15	10	90	
62		FIRST Floor	60	15	10	85	
63		FIRST Floor	60	15	10	85	
64		Second Floor	80	15	10	105	
65		Second Floor	80	15	10	105	
66		Third Floor	30	15	10	55	
67		Third Floor	30	15	10	55	
68		Fourth Floor	30	15	10	55	
69		Fourth Floor	30	15	10	55	
70		Fifth Floor	40	15	10	65	
71		Fifth Floor	40	10	10	60	
		Total	610	175	120	905	2

7.5.5 Basic Science Research Block



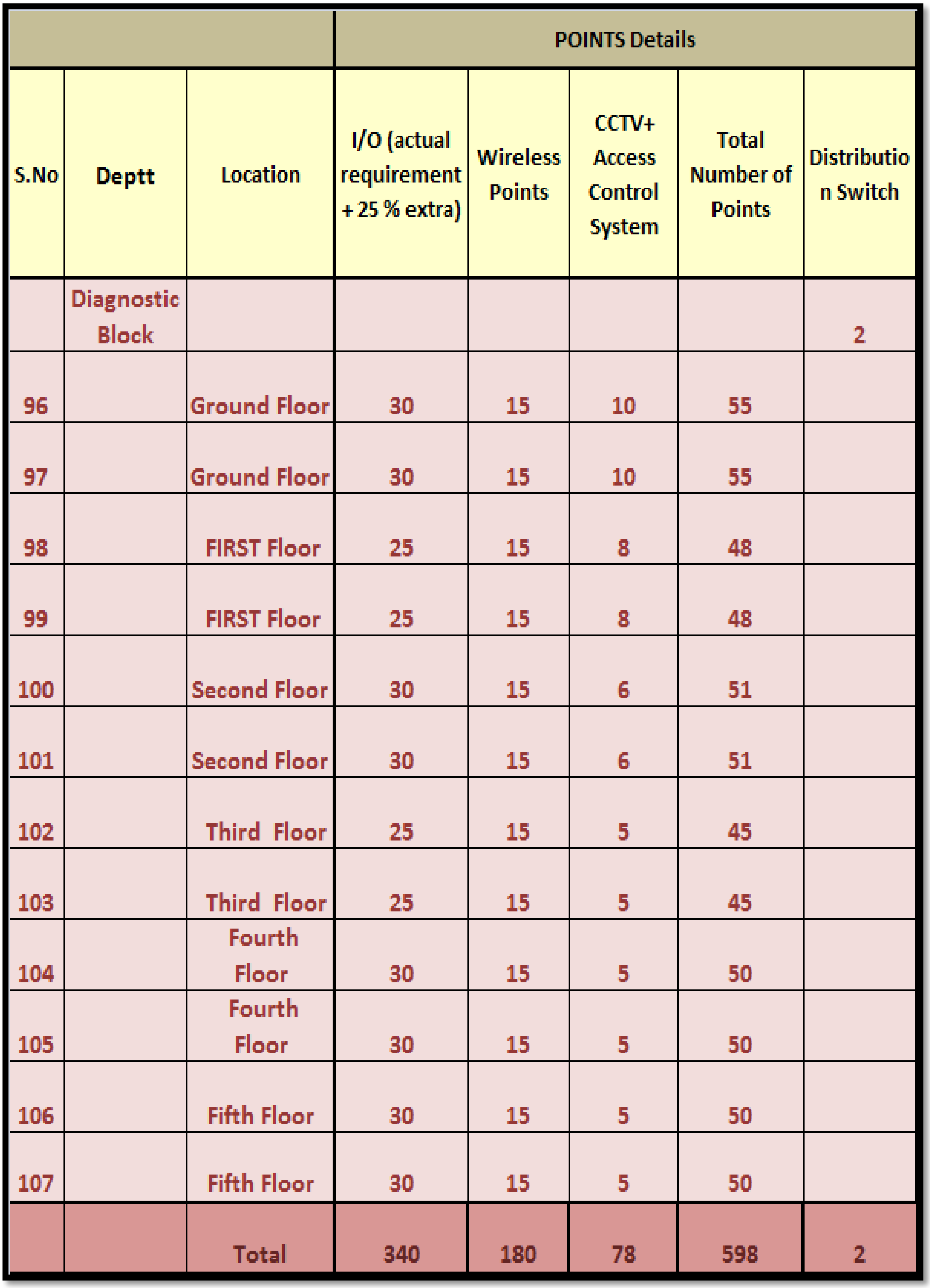
			POINTS Details				
S.No	Deptt	Location	I/O (actual requirement + 25 % extra)	Wireless Points	CCTV+ Access Control System	Total Number of Points	Distribution Switch
	Basic Science Research						2
72		Ground Floor	25	5	6	36	
73		Ground Floor	25	5	6	36	
74		FIRST Floor	25	5	6	36	
75		FIRST Floor	25	5	6	36	
76		Second Floor	25	5	6	36	
77		Second Floor	25	5	6	36	
78		Third Floor	30	5	6	41	
79		Third Floor	30	5	6	41	
80		Fourth Floor	30	5	6	41	
81		Fourth Floor	30	5	6	41	
82		Fifth Floor	30	5	6	41	
83		Fifth Floor	30	5	6	41	
		Total	330	60	72	462	2

7.5.6 Research Hostel Block



			POINTS Details				
S.No	Deptt	Location	I/O (actual requirement + 25 % extra)	Wireless Points	CCTV+ Access Control System	Total Number of Points	Distribution Switch
	Research Hostel						2
84		Ground Floor	30	15	6	51	
85		Ground Floor	30	15	6	51	
86		FIRST Floor	25	15	6	46	
87		FIRST Floor	25	15	6	46	
88		Second Floor	30	15	6	51	
89		Second Floor	30	15	6	51	
90		Third Floor	25	15	6	46	
91		Third Floor	25	15	6	46	
92		Fourth Floor	30	15	6	51	
93		Fourth Floor	30	15	6	51	
94		Fifth Floor	30	15	6	51	
95		Fifth Floor	30	15	6	51	
		Total	340	180	72	592	2

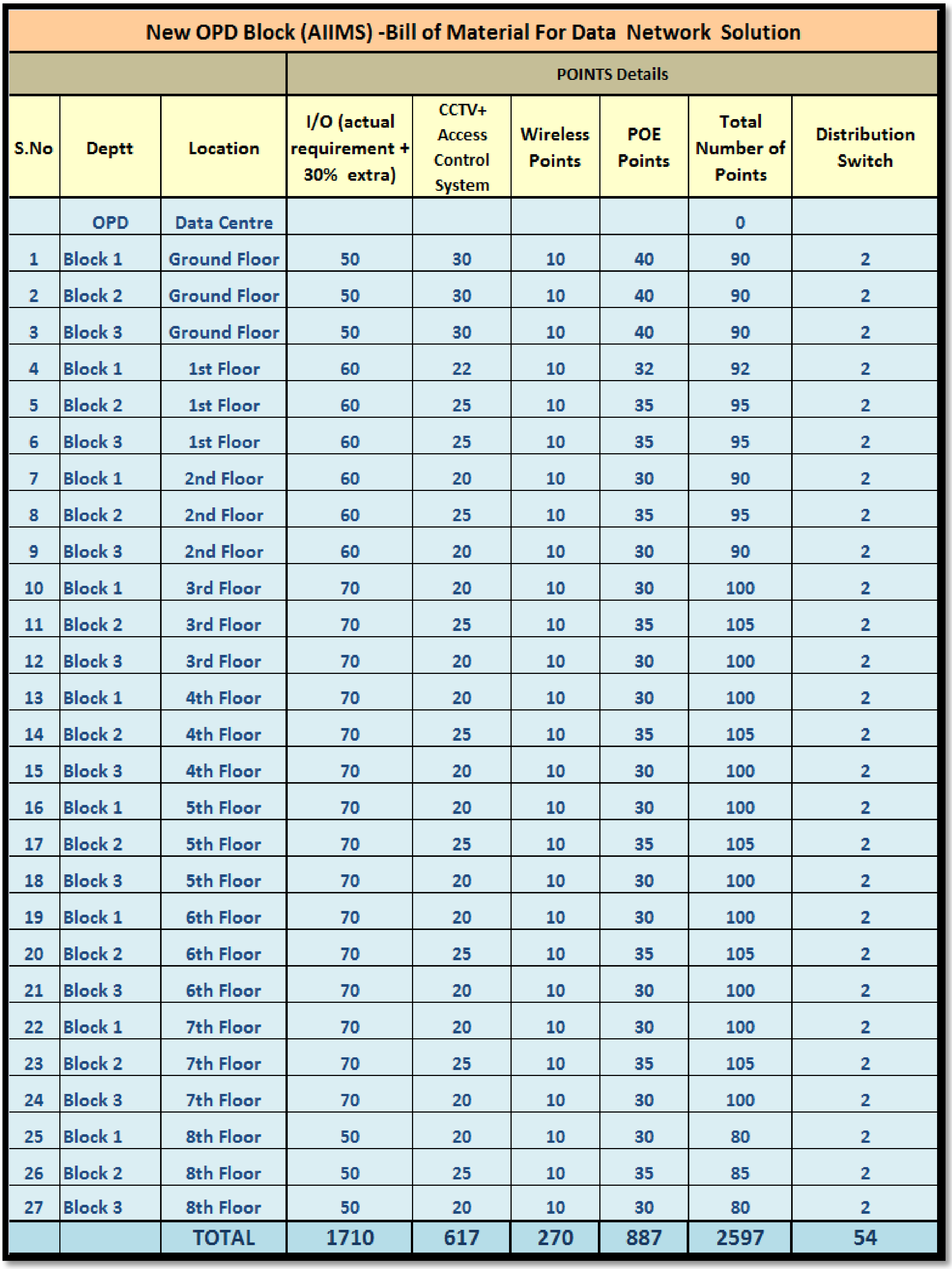
7.5.7 Diagnostic Block



			POINTS Details				
S.No	Deptt	Location	I/O (actual requirement + 25 % extra)	Wireless Points	CCTV+ Access Control System	Total Number of Points	Distribution Switch
	Diagnostic Block						2
96		Ground Floor	30	15	10	55	
97		Ground Floor	30	15	10	55	
98		FIRST Floor	25	15	8	48	
99		FIRST Floor	25	15	8	48	
100		Second Floor	30	15	6	51	
101		Second Floor	30	15	6	51	
102		Third Floor	25	15	5	45	
103		Third Floor	25	15	5	45	
104		Fourth Floor	30	15	5	50	
105		Fourth Floor	30	15	5	50	
106		Fifth Floor	30	15	5	50	
107		Fifth Floor	30	15	5	50	
		Total	340	180	78	598	2

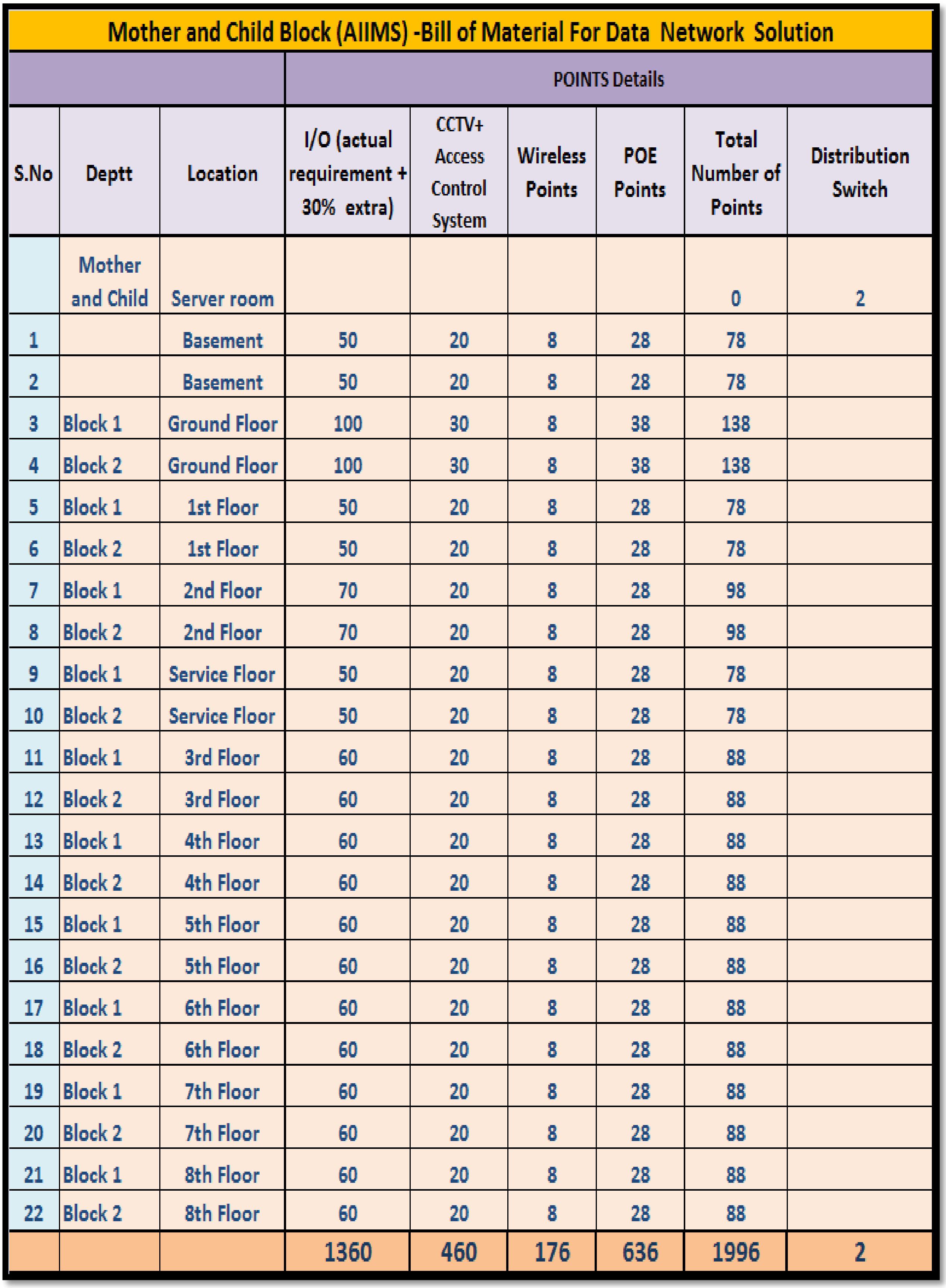
7.6 Distribution of Active and Passive items – Block wise (AIIMS, New Delhi Campus)

7.6.1 New OPD Block



New OPD Block (AIIMS) -Bill of Material For Data Network Solution								
			POINTS Details					
S.No	Deptt	Location	I/O (actual requirement + 30% extra)	CCTV+ Access Control System	Wireless Points	POE Points	Total Number of Points	Distribution Switch
	OPD	Data Centre					0	
1	Block 1	Ground Floor	50	30	10	40	90	2
2	Block 2	Ground Floor	50	30	10	40	90	2
3	Block 3	Ground Floor	50	30	10	40	90	2
4	Block 1	1st Floor	60	22	10	32	92	2
5	Block 2	1st Floor	60	25	10	35	95	2
6	Block 3	1st Floor	60	25	10	35	95	2
7	Block 1	2nd Floor	60	20	10	30	90	2
8	Block 2	2nd Floor	60	25	10	35	95	2
9	Block 3	2nd Floor	60	20	10	30	90	2
10	Block 1	3rd Floor	70	20	10	30	100	2
11	Block 2	3rd Floor	70	25	10	35	105	2
12	Block 3	3rd Floor	70	20	10	30	100	2
13	Block 1	4th Floor	70	20	10	30	100	2
14	Block 2	4th Floor	70	25	10	35	105	2
15	Block 3	4th Floor	70	20	10	30	100	2
16	Block 1	5th Floor	70	20	10	30	100	2
17	Block 2	5th Floor	70	25	10	35	105	2
18	Block 3	5th Floor	70	20	10	30	100	2
19	Block 1	6th Floor	70	20	10	30	100	2
20	Block 2	6th Floor	70	25	10	35	105	2
21	Block 3	6th Floor	70	20	10	30	100	2
22	Block 1	7th Floor	70	20	10	30	100	2
23	Block 2	7th Floor	70	25	10	35	105	2
24	Block 3	7th Floor	70	20	10	30	100	2
25	Block 1	8th Floor	50	20	10	30	80	2
26	Block 2	8th Floor	50	25	10	35	85	2
27	Block 3	8th Floor	50	20	10	30	80	2
		TOTAL	1710	617	270	887	2597	54

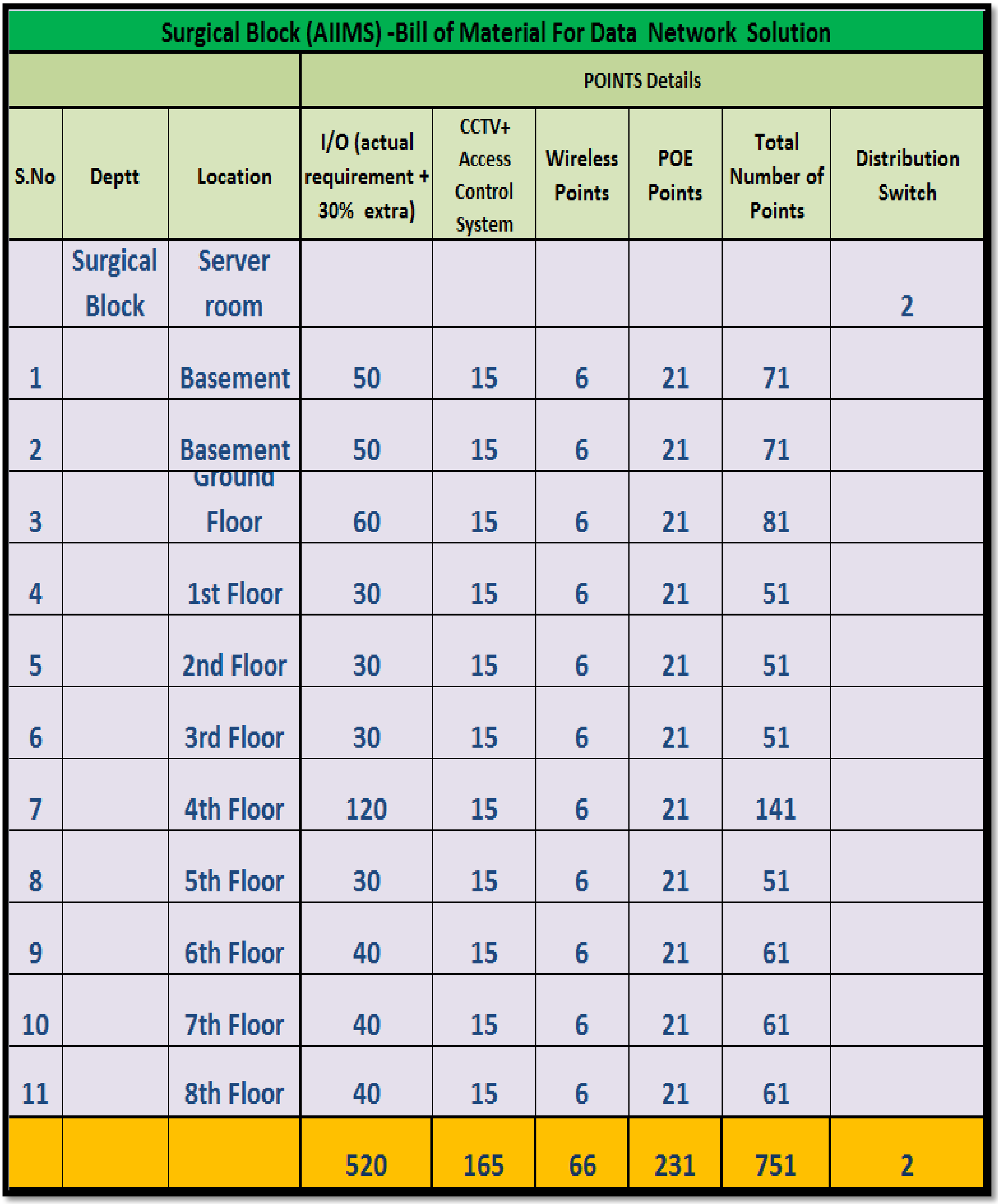
7.6.2 Mother and Child Block



Mother and Child Block (AIIMS) -Bill of Material For Data Network Solution

			POINTS Details					
S.No	Deptt	Location	I/O (actual requirement + 30% extra)	CCTV+ Access Control System	Wireless Points	POE Points	Total Number of Points	Distribution Switch
	Mother and Child	Server room					0	2
1		Basement	50	20	8	28	78	
2		Basement	50	20	8	28	78	
3	Block 1	Ground Floor	100	30	8	38	138	
4	Block 2	Ground Floor	100	30	8	38	138	
5	Block 1	1st Floor	50	20	8	28	78	
6	Block 2	1st Floor	50	20	8	28	78	
7	Block 1	2nd Floor	70	20	8	28	98	
8	Block 2	2nd Floor	70	20	8	28	98	
9	Block 1	Service Floor	50	20	8	28	78	
10	Block 2	Service Floor	50	20	8	28	78	
11	Block 1	3rd Floor	60	20	8	28	88	
12	Block 2	3rd Floor	60	20	8	28	88	
13	Block 1	4th Floor	60	20	8	28	88	
14	Block 2	4th Floor	60	20	8	28	88	
15	Block 1	5th Floor	60	20	8	28	88	
16	Block 2	5th Floor	60	20	8	28	88	
17	Block 1	6th Floor	60	20	8	28	88	
18	Block 2	6th Floor	60	20	8	28	88	
19	Block 1	7th Floor	60	20	8	28	88	
20	Block 2	7th Floor	60	20	8	28	88	
21	Block 1	8th Floor	60	20	8	28	88	
22	Block 2	8th Floor	60	20	8	28	88	
			1360	460	176	636	1996	2

7.6.3 Surgical Block

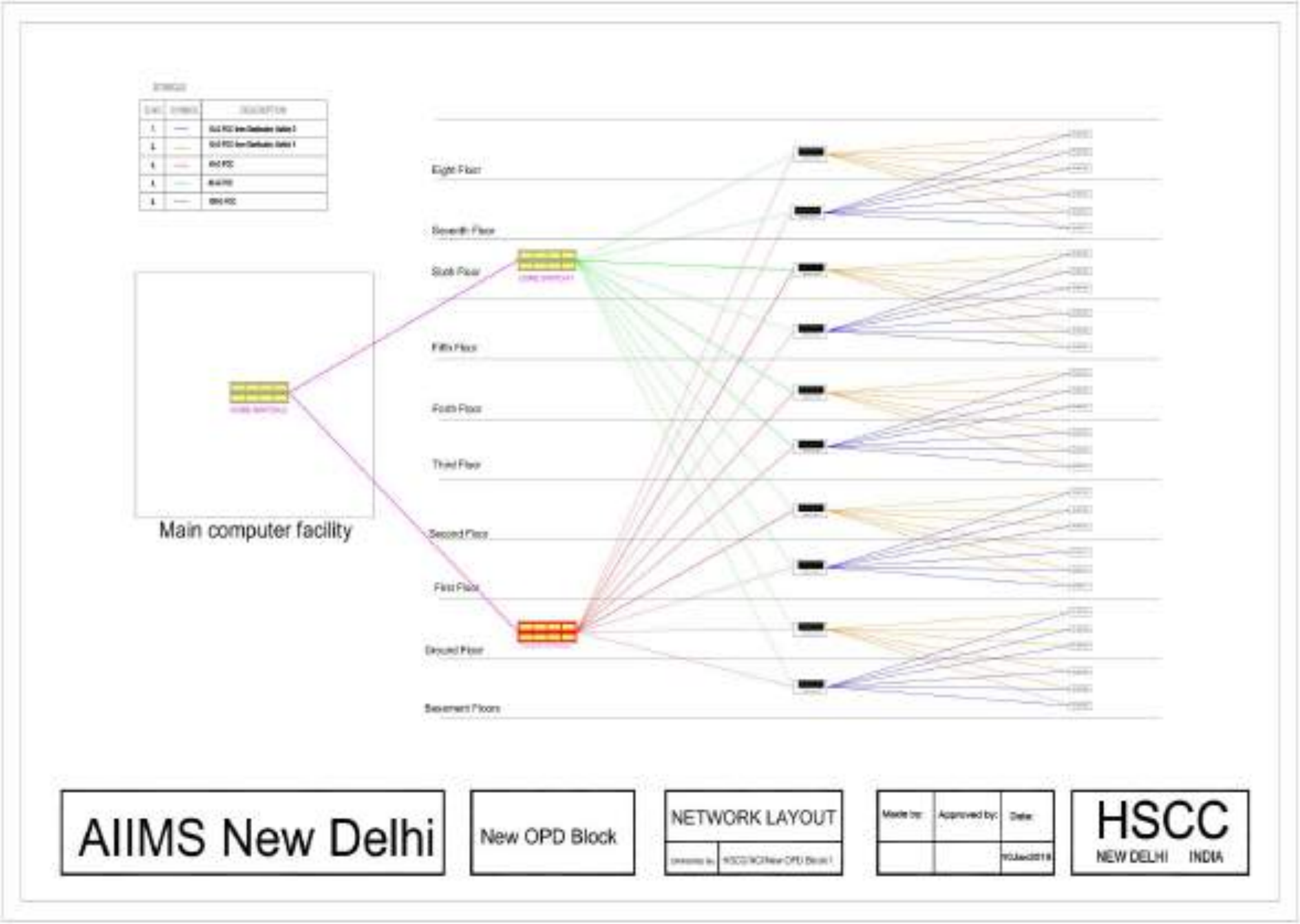


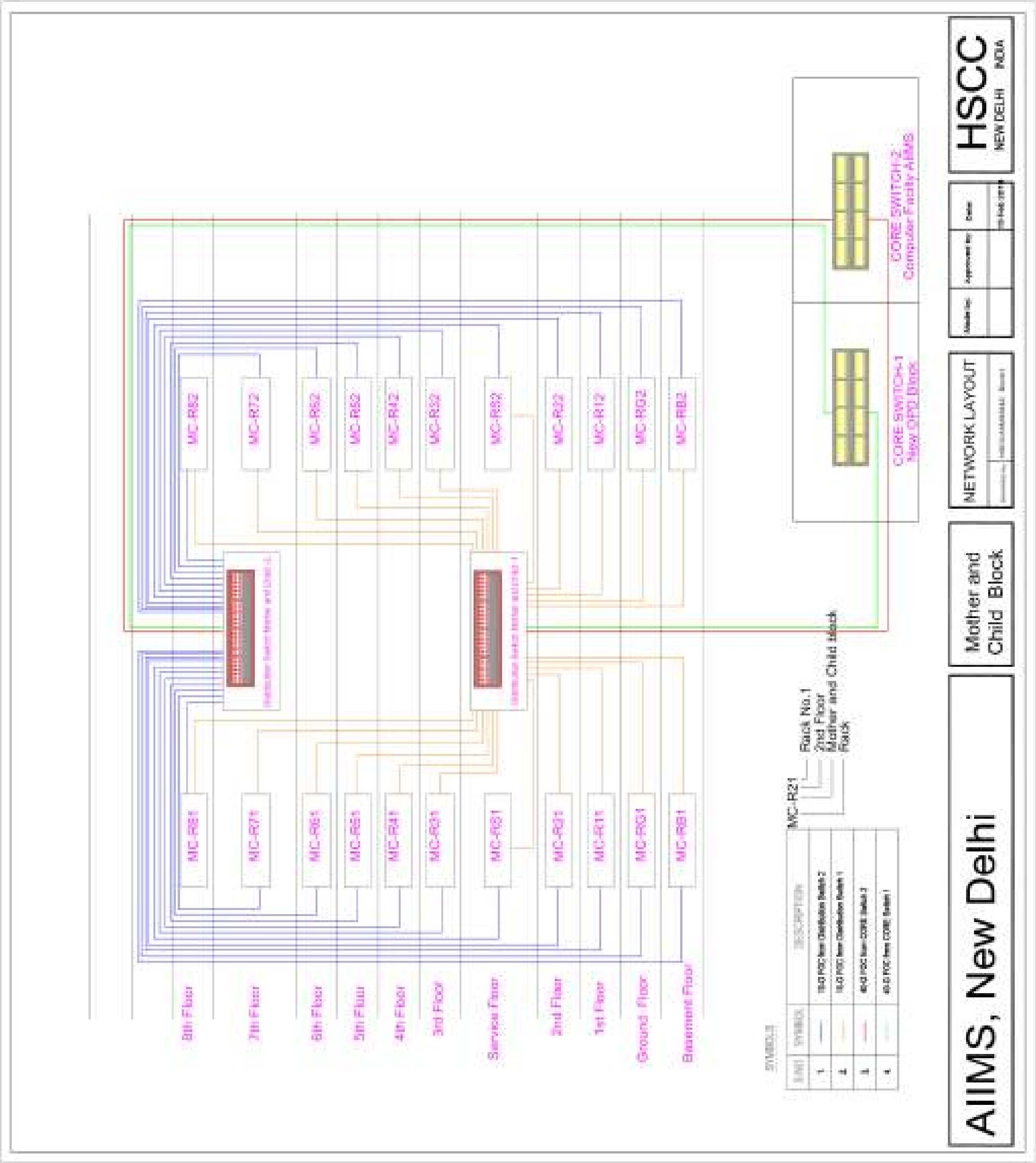
Surgical Block (AIIMS) -Bill of Material For Data Network Solution								
			POINTS Details					
S.No	Deptt	Location	I/O (actual requirement + 30% extra)	CCTV+ Access Control System	Wireless Points	POE Points	Total Number of Points	Distribution Switch
	Surgical Block	Server room						2
1		Basement	50	15	6	21	71	
2		Basement	50	15	6	21	71	
3		Ground Floor	60	15	6	21	81	
4		1st Floor	30	15	6	21	51	
5		2nd Floor	30	15	6	21	51	
6		3rd Floor	30	15	6	21	51	
7		4th Floor	120	15	6	21	141	
8		5th Floor	30	15	6	21	51	
9		6th Floor	40	15	6	21	61	
10		7th Floor	40	15	6	21	61	
11		8th Floor	40	15	6	21	61	
			520	165	66	231	751	2

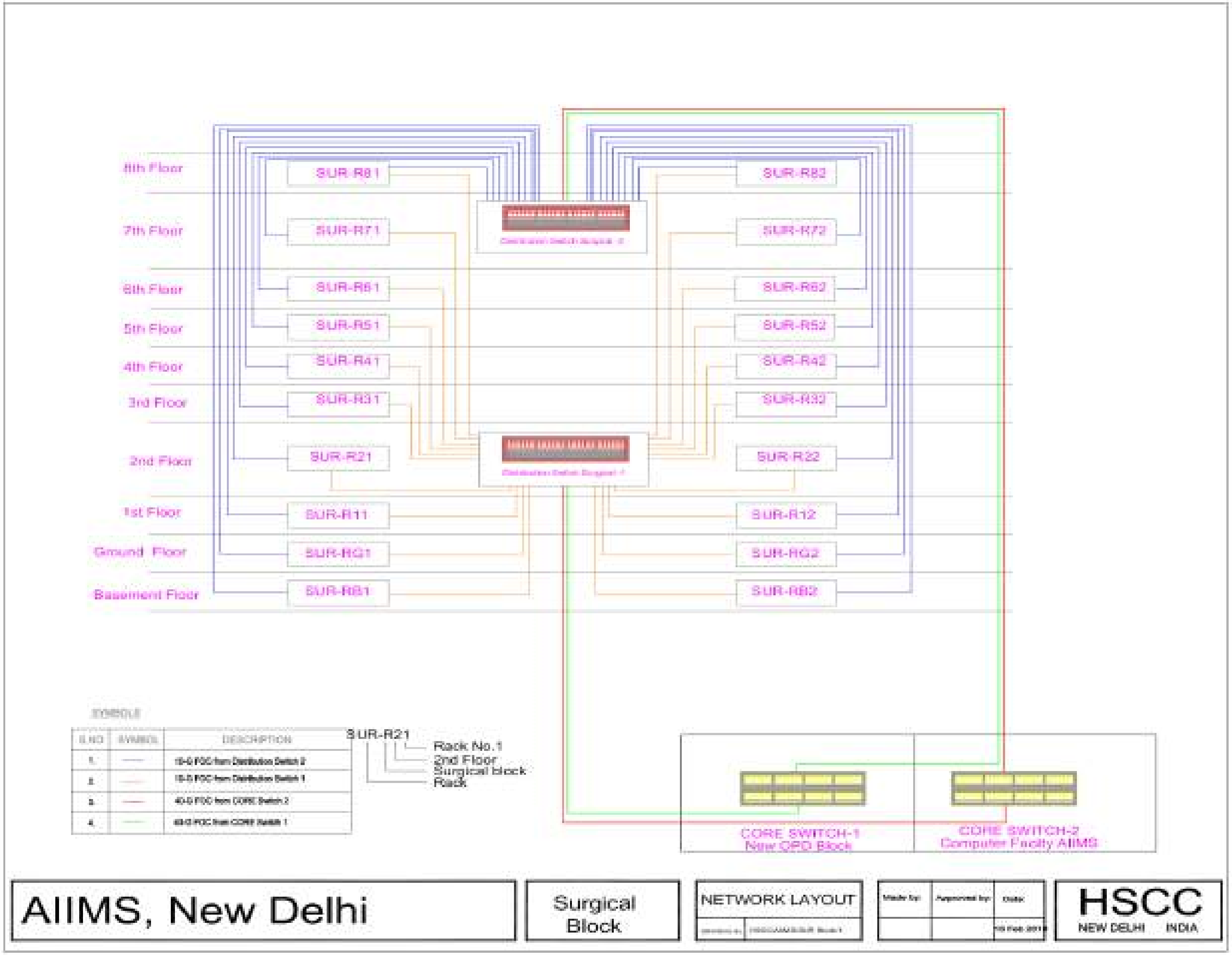
Annexure-B

7.7 Proposed Network diagrams

AIIMS New Delhi Campus


Eight Floor
Seventh Floor
Sixth Floor
Fifth Floor
Forth Floor
Third Floor
Second Floor
First Floor
Ground Floor
Basement Floors
Main computer facility
AIIMS New Delhi
New OPD Block
NETWORK LAYOUT
Made by:
Approved by:
Date:
HSCC
NEW DELHI INDIA

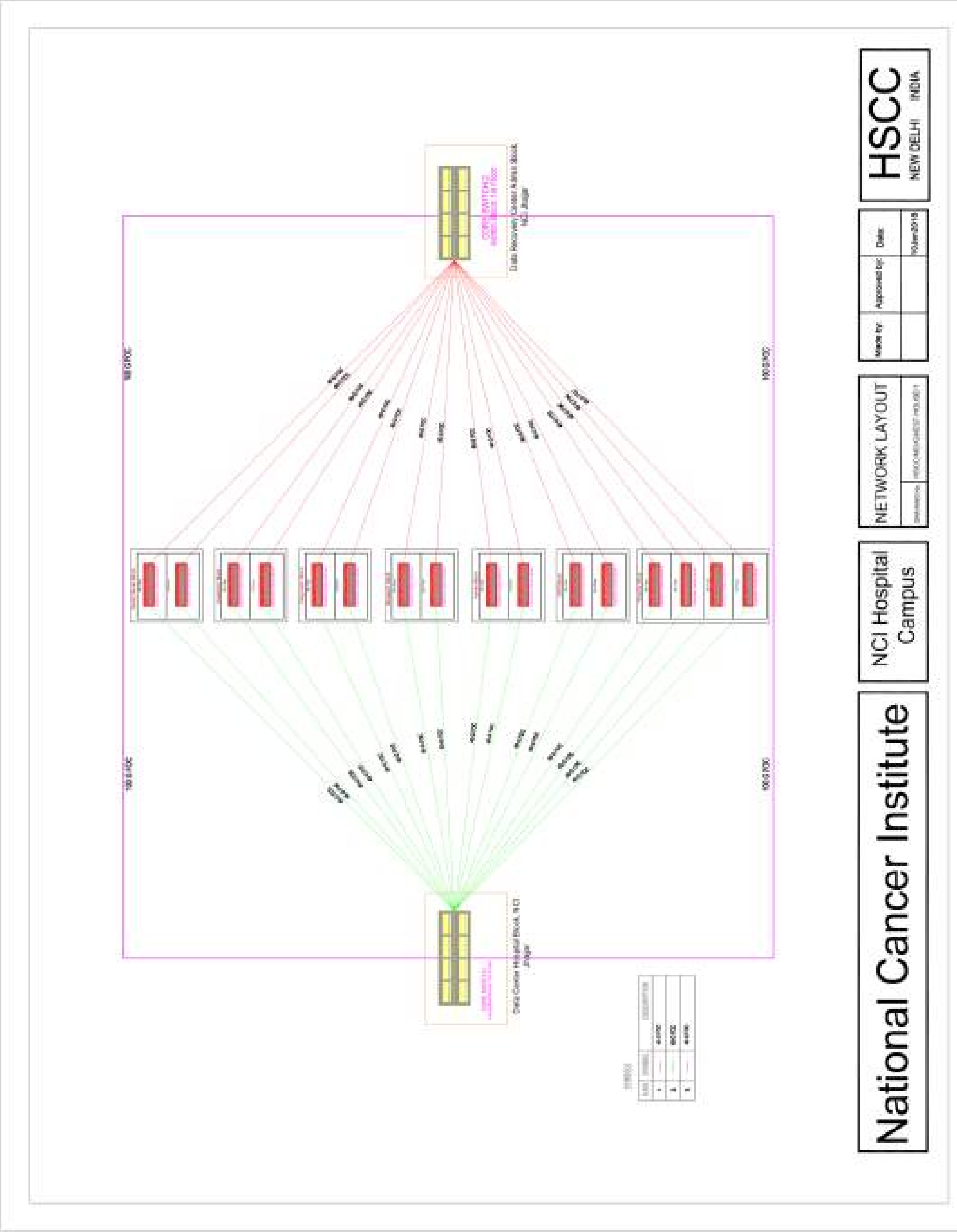

8th Floor
7th Floor
6th Floor
5th Floor
4th Floor
3rd Floor
Service Floor
2nd Floor
1st Floor
Ground Floor
Basement Floor
MC-R81
MC-R71
MC-R61
MC-R51
MC-R41
MC-R31
MC-RS1
MC-R21
MC-R11
MC-RG1
MC-RB1
MC-R82
MC-R72
MC-R62
MC-R52
MC-R42
MC-R32
MC-RS2
MC-R22
MC-R12
MC-RG2
MC-RB2
MC-R21
Rack No.1
2nd Floor
Mother and Child block
Rack
CORE SWITCH-1
New OPD Block
CORE SWITCH-2
Computer Facility AIIMS
SYMBOLS
SYMBOL
DESCRIPTION
1
1
1
1
NETWORK LAYOUT
Mother and Child Block
AIIMS, New Delhi
HSCC
NEW DELHI INDIA

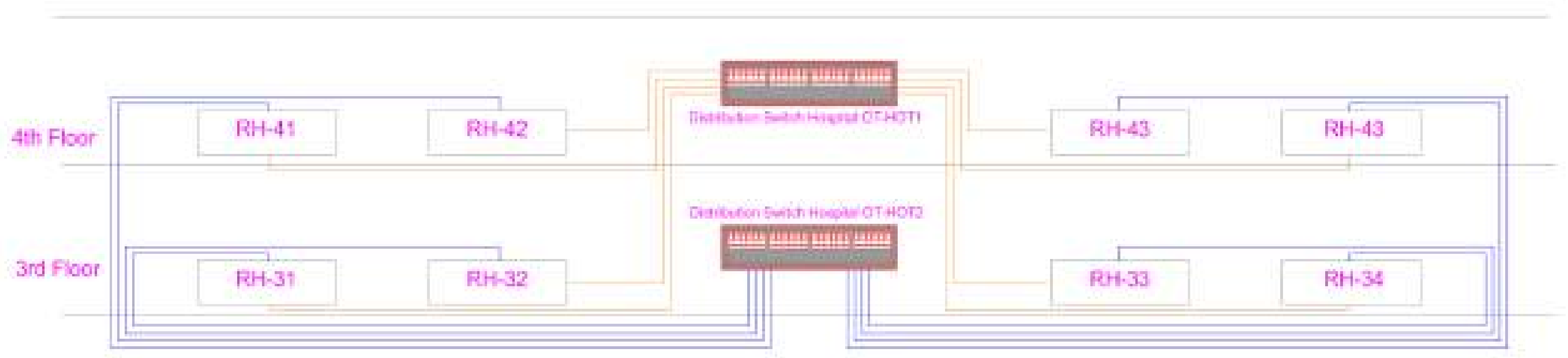


SYMBOLS

S.NO	SYMBOL	DESCRIPTION
1.	—	10-G FOC from Distribution Switch 2
2.	—	10-G FOC from Distribution Switch 1
3.	—	40-G FOC from CORE Switch 2
4.	—	40-G FOC from CORE Switch 1

NCI Jhajjar Campus –


National Cancer Institute
NCI Hospital Campus
NETWORK LAYOUT
Made by:
Approved by:
Date:
HSCC
NEW DELHI INDIA


4th Floor
3rd Floor
RH-41
RH-42
RH-43
RH-43
RH-31
RH-32
RH-33
RH-34
Distribution Switch Hospital OT-HOT1
Distribution Switch Hospital OT-HOT2

SYMBOLS

S.NO	SYMBOL	DESCRIPTION
1.	—	10-G FOC from Distribution Switch 2
2.	—	10-G FOC from Distribution Switch 1
3.	—	40-G FOC from CORE Switch 2
4.	—	40-G FOC from CORE Switch 1

RH-G1
Rack No.1
Ground Floor
Hospital block
Rack

RH-21
Rack No.1
2nd Floor
Hospital block
Rack

RH-B1
Rack No.1
Basement Floor
Hospital block
Rack

(Distribution Switch to Access Switch)

National Cancer Institute

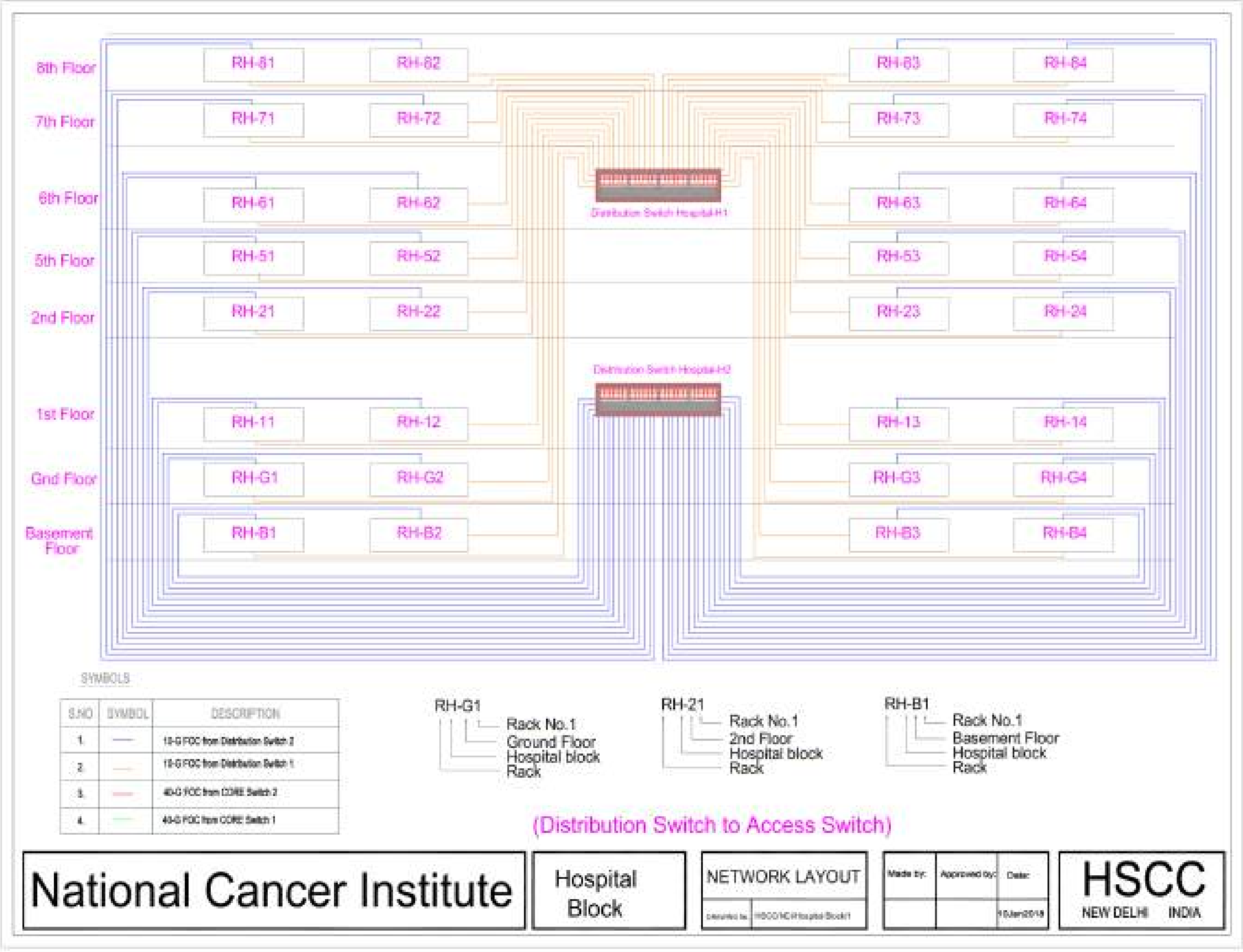
Hospital
Block-OT

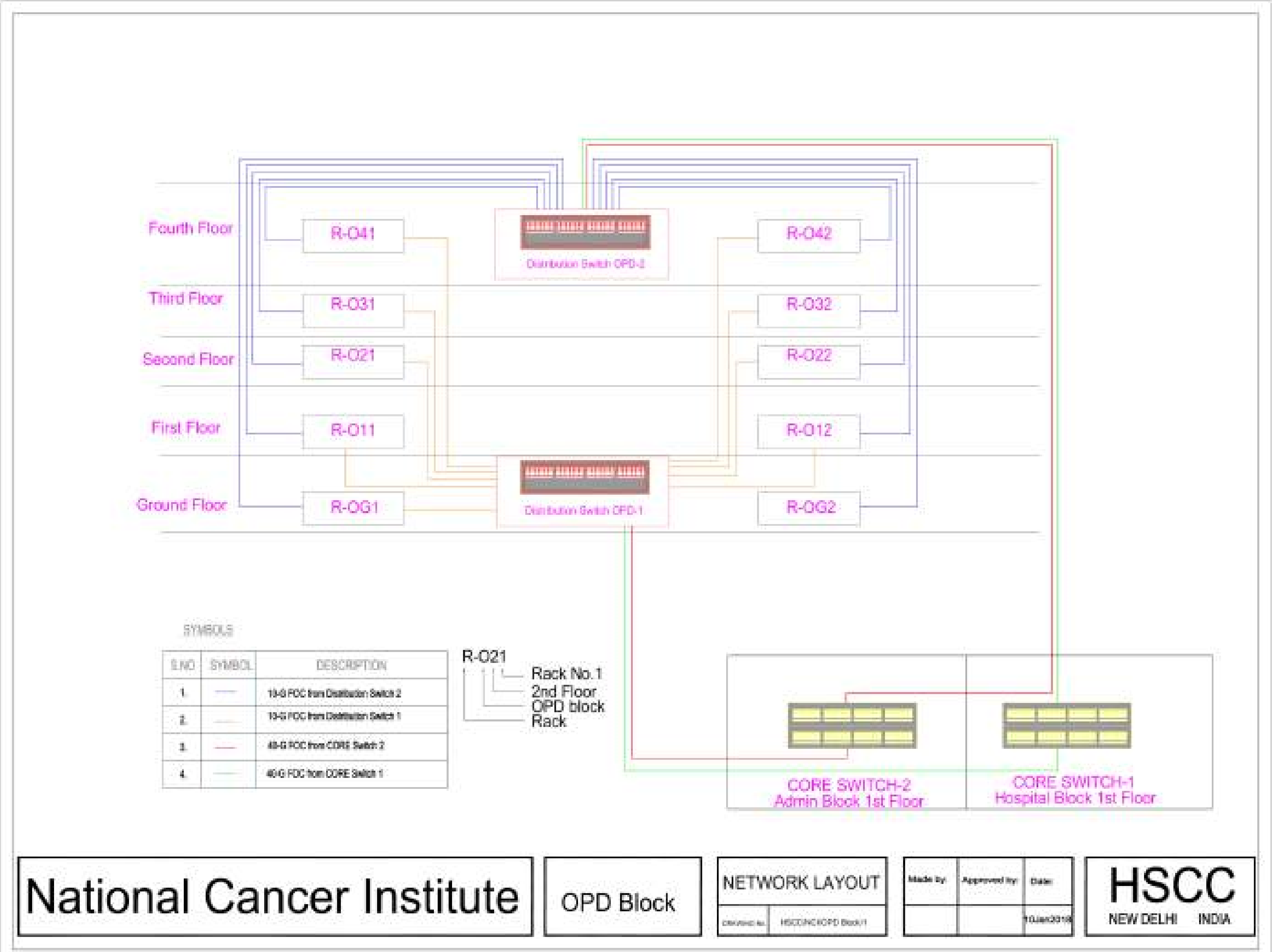
NETWORK LAYOUT

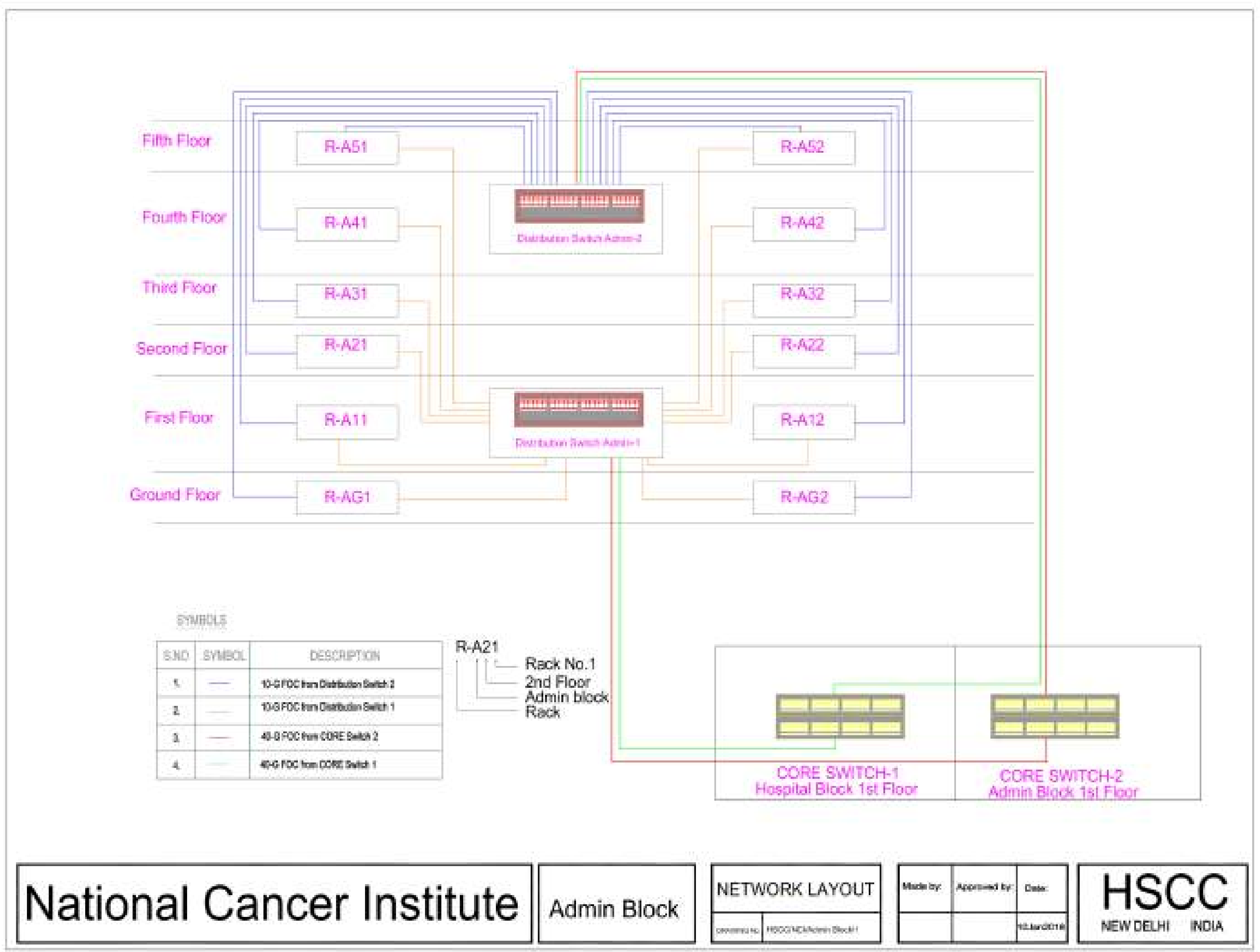
Drg. No.	HSCC/NCI/Hospital Block/2

Made by:	Approved by:	Date:
		10Jan2018

HSCC
NEW DELHI INDIA

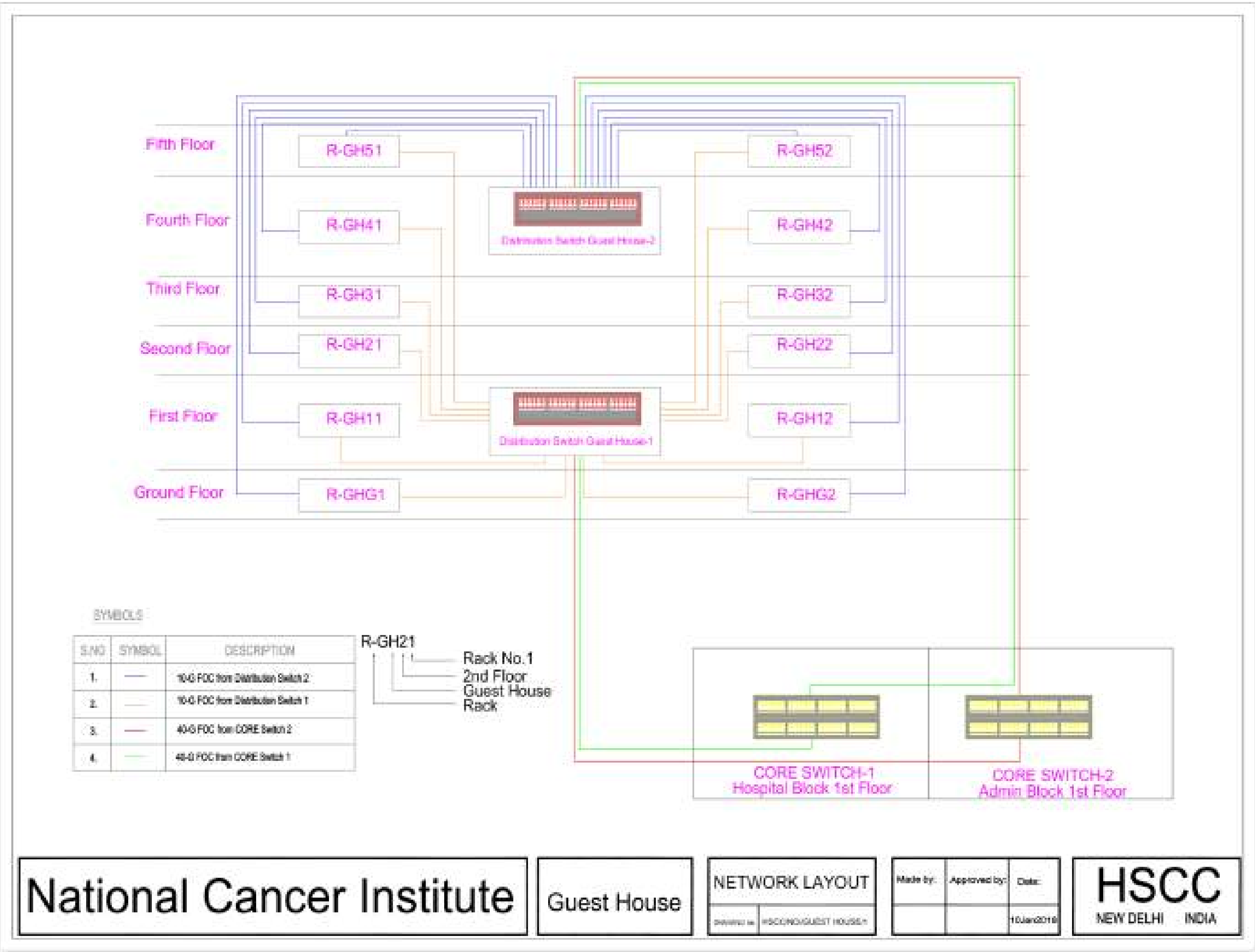

8th Floor
7th Floor
6th Floor
5th Floor
2nd Floor
1st Floor
Gnd Floor
Basement Floor
RH-81
RH-82
RH-83
RH-84
RH-71
RH-72
RH-73
RH-74
RH-61
RH-62
RH-63
RH-64
RH-51
RH-52
RH-53
RH-54
RH-21
RH-22
RH-23
RH-24
RH-11
RH-12
RH-13
RH-14
RH-G1
RH-G2
RH-G3
RH-G4
RH-B1
RH-B2
RH-B3
RH-B4
Distribution Switch Hospital-H1
Distribution Switch Hospital-H2
SYMBOLS
S.NO
SYMBOL
DESCRIPTION
1.
10-G FOC from Distribution Switch 2
2.
10-G FOC from Distribution Switch 1
3.
40-G FOC from CORE Switch 2
4.
40-G FOC from CORE Switch 1
RH-G1
Rack No.1
Ground Floor
Hospital block
Rack
RH-21
Rack No.1
2nd Floor
Hospital block
Rack
RH-B1
Rack No.1
Basement Floor
Hospital block
Rack
(Distribution Switch to Access Switch)
National Cancer Institute
Hospital Block
NETWORK LAYOUT
Drawing No.
HSCC/NCI/Hospital Block1
Made by:
Approved by:
Date:
10Jan2018
HSCC
NEW DELHI
INDIA

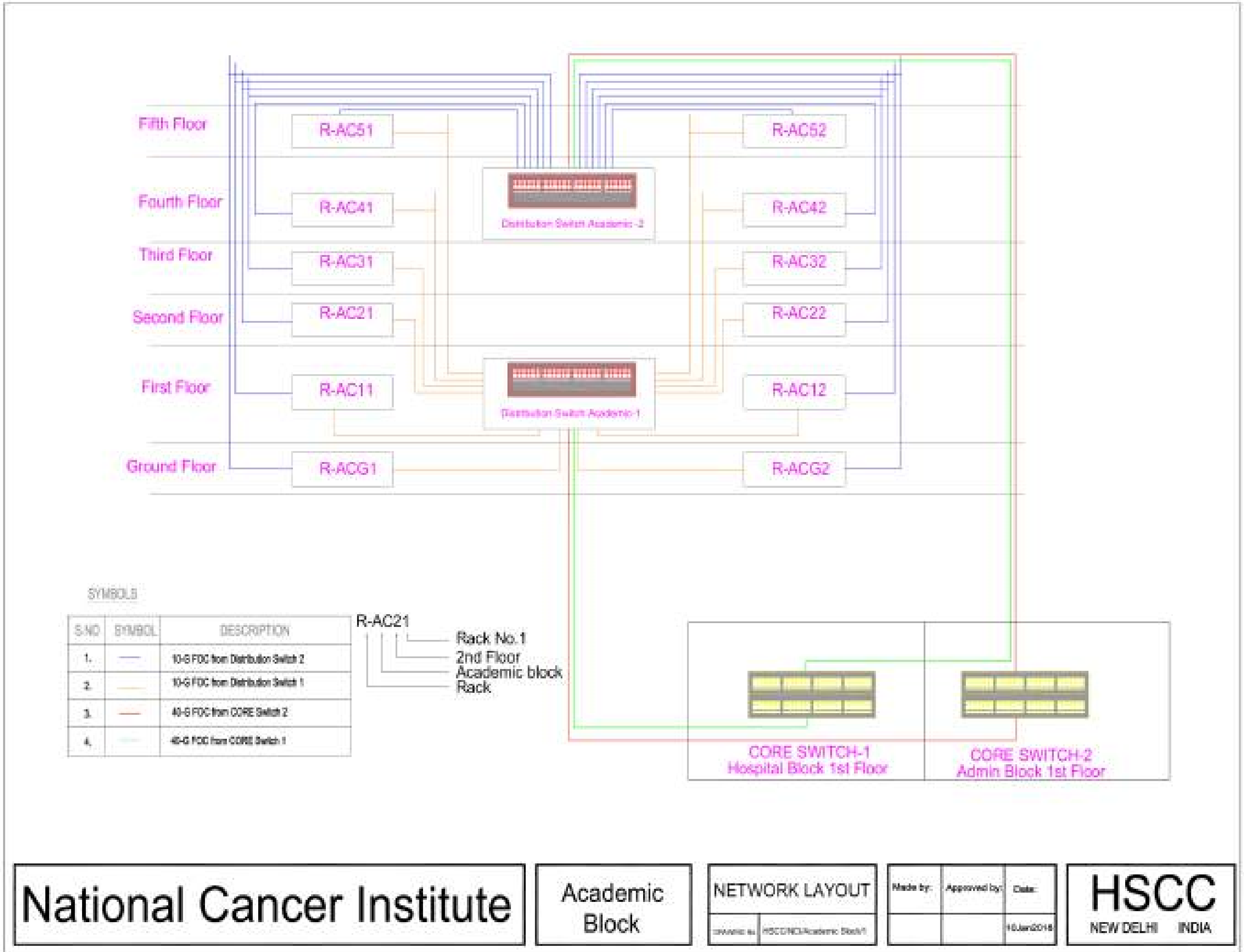

Fourth Floor
Third Floor
Second Floor
First Floor
Ground Floor
R-O41
R-O31
R-O21
R-O11
R-OG1
R-O42
R-O32
R-O22
R-O12
R-OG2
Distribution Switch OPD-2
Distribution Switch OPD-1
CORE SWITCH-2
Admin Block 1st Floor
CORE SWITCH-1
Hospital Block 1st Floor
SYMBOLS
S.NO
SYMBOL
DESCRIPTION
1.
10-G FOC from Distribution Switch 2
2.
10-G FOC from Distribution Switch 1
3.
40-G FOC from CORE Switch 2
4.
40-G FOC from CORE Switch 1
R-O21
Rack No.1
2nd Floor
OPD block
Rack
National Cancer Institute
OPD Block
NETWORK LAYOUT
Drawing No.
HSCC/NCI/OPD Block/1
Made by:
Approved by:
Date:
10Jan2018
HSCC
NEW DELHI
INDIA



SYMBOLS

S.NO	SYMBOL	DESCRIPTION
1.	—	10-G FOC from Distribution Switch 2
2.	—	10-G FOC from Distribution Switch 1
3.	—	40-G FOC from CORE Switch 2
4.	—	40-G FOC from CORE Switch 1


Fifth Floor
Fourth Floor
Third Floor
Second Floor
First Floor
Ground Floor
R-GH51
R-GH41
R-GH31
R-GH21
R-GH11
R-GHG1
R-GH52
R-GH42
R-GH32
R-GH22
R-GH12
R-GHG2
Distribution Switch Guest House-2
Distribution Switch Guest House-1
CORE SWITCH-1
Hospital Block 1st Floor
CORE SWITCH-2
Admin Block 1st Floor
SYMBOLS
S.NO
SYMBOL
DESCRIPTION
1.
10-G FOC from Distribution Switch 2
2.
10-G FOC from Distribution Switch 1
3.
40-G FOC from CORE Switch 2
4.
40-G FOC from CORE Switch 1
R-GH21
Rack No.1
2nd Floor
Guest House
Rack
National Cancer Institute
Guest House
NETWORK LAYOUT
Drawing no.
HSCC/NCI/GUEST HOUSE-1
Made by:
Approved by:
Date:
10Jan2018
HSCC
NEW DELHI
INDIA



SYMBOLS

S.NO	SYMBOL	DESCRIPTION
1.	—	10-G FOC from Distribution Switch 2
2.	—	10-G FOC from Distribution Switch 1
3.	—	40-G FOC from CORE Switch 2
4.	—	40-G FOC from CORE Switch 1

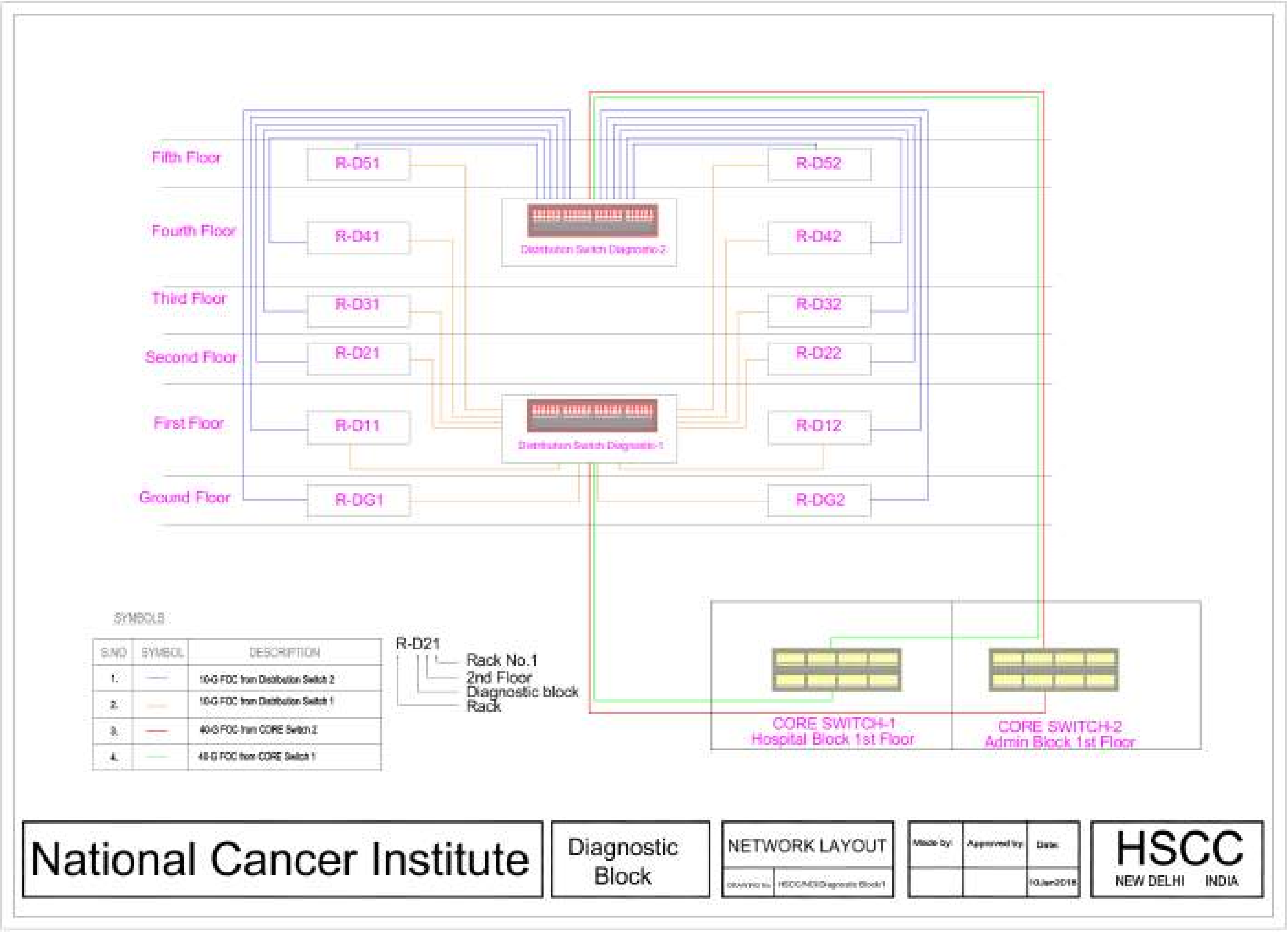
National Cancer Institute

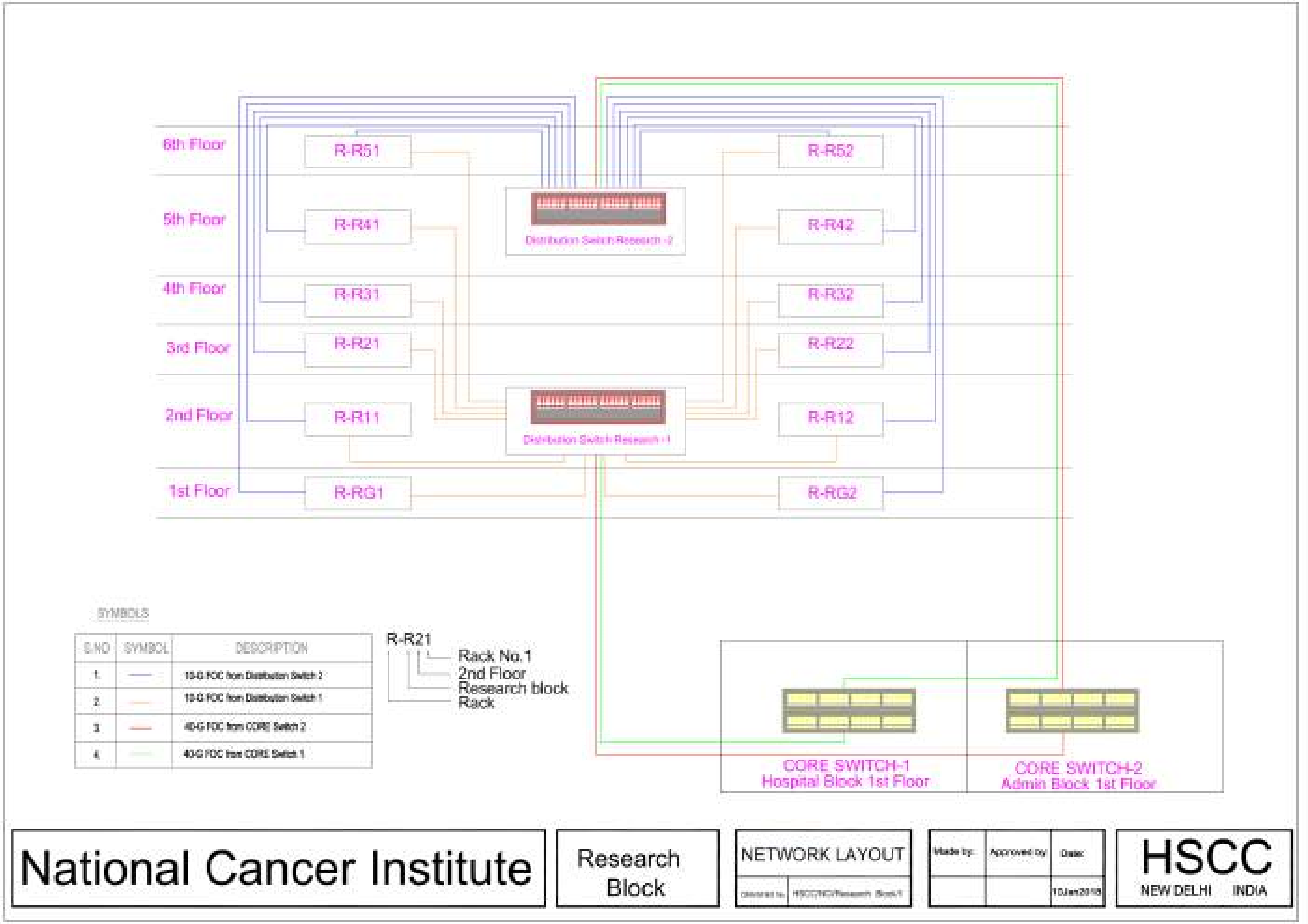
Academic Block

NETWORK LAYOUT

Drawing no.	HSCC/NCI/Academic Block/1	Made by:	Approved by:	Date:
				10Jan2018

HSCC
NEW DELHI INDIA


Fifth Floor
Fourth Floor
Third Floor
Second Floor
First Floor
Ground Floor
R-D51
R-D41
R-D31
R-D21
R-D11
R-DG1
R-D52
R-D42
R-D32
R-D22
R-D12
R-DG2
Distribution Switch Diagnostic-2
Distribution Switch Diagnostic-1
CORE SWITCH-1
Hospital Block 1st Floor
CORE SWITCH-2
Admin Block 1st Floor
SYMBOLS
S.NO
SYMBOL
DESCRIPTION
1.
10-G FOC from Distribution Switch 2
2.
10-G FOC from Distribution Switch 1
3.
40-G FOC from CORE Switch 2
4.
40-G FOC from CORE Switch 1
R-D21
Rack No.1
2nd Floor
Diagnostic block
Rack
National Cancer Institute
Diagnostic
Block
NETWORK LAYOUT
DRAWING No.
HSCC/NCI/Diagnostic Block/1
Made by:
Approved by:
Date:
10Jan2018
HSCC
NEW DELHI
INDIA



SYMBOLS

S.NO	SYMBOL	DESCRIPTION
1.	—	10-G FOC from Distribution Switch 2
2.	—	10-G FOC from Distribution Switch 1
3.	—	40-G FOC from CORE Switch 2
4.	—	40-G FOC from CORE Switch 1

National Cancer Institute

Research Block

NETWORK LAYOUT

Drawing No. HSCC/NCI/Research Block-1

Made by:	Approved by:	Date:
		10Jan2018

HSCC
NEW DELHI INDIA

Annexure-C

(Technical Specification for Active devices and Passive devices)

7.8 Technical Specification for Active devices and Passive devices

General Criteria-

- Switches: All Switches (Core, Distribution and Access) and Transceivers should be of same OEM.
- All Active components and passive components and Operations and maintenance services should be quoted with minimum 5 years warranty including 24 X 7 Technical Assistance support. Price of CAMC for a period of 5 years after completion of warranty should be quoted.
- The Access Switches should support link aggregation across the stack.
- All Switches should be manageable from the same NMS.
- All Core switches and Distribution switches must have dual redundant hot-swappable power supply.
- All switches should have inbuilt support for 802.3az/ Energy Efficient Ethernet/ Green Ethernet.
- All Switches should be configured to provide Wire-Speed Non-Blocking Switching.
- OEM must have direct support centre in India and must have direct support Infrastructure.
- OEM shall have ISO 9001 certification
- The Bidder will specify exactly (not more than, not less than) ONE make and model of the product offered against each specified BOQ item.

1. Core Switch

Sr. no.	Specification
1	Core Switch should be configurable in a High Availability (Active-Active) mode with support for dual homing connections.
2	Core switch should be configured with appropriate supervisory hardware with redundancy in power supplies and fans.
3	Core Switch should be configured to provide Wire-Speed Non-Blocking Switching, distributed forwarding and Routing Performance at Layer 2 and Layer 3 on all ports.
4	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
5	Each Core Switch should have minimum 4x100G, 40 ports of 40G QSFP and min 24 Ports 10G SFP+ wire speed from day 1.
6	The ports on each core switch should be capable of supporting 1000Base-TX/1000Base-LX and 10G, 40G Direct-Attached Copper, 40G SR and 40G LR SFP+ connectivity options.

7	It should support Unicast, Multicast routing and IPv4 and IPv6 routes.
8	Switch should support IEEE for user authentications, accounting, RADIUS and TACACS.
9	The Core Switches should support min 64K MAC addresses and min 4K active VLANs.
10	The Core Switches should support full Layer 2 features like STP, RSTP, MSTP, LAG, LACP, ACL, QoS and IGMPv1/v2 from day 1..
11	The Core Switches should support full Layer 3 features like PIM-DM/SM, OSPF, VRRP, PBR and BGP from day 1
12	TheCoreSwitchesshouldsupportfullIPv6featureslikeMLDv1/v2, OSPFv3, VRRPv3, BGP4+ and IPv6 management from day 1.
13	Should support security features like standard / extended ACLs, based on port and/ or time.
14	The switch should have control plane policing feature to filter the unwanted traffic entering the CPU queues.
15	Should support MAC address filtering based on source and destination addresses.
16	The switch should support Non Stop Routing (NSR) / NSF / Graceful Restart/Hitless failover.
17	Each core switch must have Virtual Output Queuing or have minimum 8 or more Hardware QoS Queues to avoid head of line blocking/prioritizing multicast for live streaming in critical applications like PACS, HMIS, CCTV etc.
18	Switch should support CLI, SSHv2, telnet for management
19	The Core Switch should support SNMP v1, v2 & v3 for management. It should bemanageable with any standard EMS/NMS.

2. Distribution Switch- Type 1

Sr. No.	Specifications
1	The switch should have Dual hot-swappable power supplies.
2	Switch should have 48 x10G SFP+ ports.

3	The switch shall have 2x 40G QSFP+ ports.
4	Shall be 19" Rack Mountable.
5	1 RJ-45 serial console port.
6	The switch should support full Layer 2 & Layer 3 features like STP, RSTP, MSTP,VLAN, LAG, LACP, ACL, QoS, OSPF and IGMPv1/v2 from day 1.
7	Switch should support integration with RADIUS/ TACACS+ authentication servers.
8	Switch should support CLI, SSHv2, and telnet for Management.

3. Distribution Switch- Type 2

Sr. No.	Specifications
1	The switch should have Dual hot-swappable power supplies.
2	Switch should have 24 x10G SFP+ ports.
3	The switch shall have 2x 40G QSFP+ ports.
4	Shall be 19" Rack Mountable.
5	1 RJ-45 serial console port.
6	The switch should support full Layer 2 & Layer 3 features like STP, RSTP, MSTP,VLAN, LAG, LACP, ACL, QoS, OSPF and IGMPv1/v2 from day 1.
7	Switch should support integration with RADIUS/ TACACS+ authentication servers.
8	Switch should support CLI, SSHv2, and telnet for Management.

4. Distribution Switch- Type 3

Sr. No.	Specifications
1	The switch should have Dual hot-swappable power supplies.
2	Switch should have 12 x10G SFP+ ports.
3	The switch shall have 2x 40G QSFP+ ports.
4	Shall be 19" Rack Mountable.

5	1 RJ-45 serial console port.
6	The switch should support full Layer 2 & Layer 3 features like STP, RSTP, MSTP,VLAN, LAG, LACP, ACL, QoS, OSPF and IGMPv1/v2 from day 1.
7	Switch should support integration with RADIUS/ TACACS+ authentication servers.
8	Switch should support CLI, SSHv2, and telnet for Management.

5. Distribution Switch- Type 4

Sr. No.	Specifications
1	The switch should have Dual hot-swappable power supplies.
2	Switch should have minimum 6 x10G SFP+ ports and 6x 10G 10G Base-T ports
3	The switch shall have 2x 40G QSFP+ ports.
4	Shall be 19" Rack Mountable.
5	1 RJ-45 serial console port.
6	The switch should support full Layer 2 & Layer 3 features like STP, RSTP, MSTP,VLAN, LAG, LACP, ACL, QoS, OSPF and IGMPv1/v2 from day 1.
7	Switch should support integration with RADIUS/ TACACS+ authentication servers.
8	Switch should support CLI, SSHv2, and telnet for Management.

6. Access Switch 24 Port

Sr. No.	Specifications
1	Access Switch should have 24 ports of 100/1000 RJ45 and minimum 2 ports of 10G (2 SFP+ for uplink).
2	The Access switch should support VLANs.
3	The Access Switch should support minimum stacking up to 4 units. Cost of the stacking modules/Ports should be included.

4	The Access Switches should support link aggregation across the stack.
5	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
6	The Access Switch should support full Layer 2 features like STP, RSTP, MSTP, LAG, LACP, ACL, QoS.
7	The Access Switch should support basic L2 features like IPv4 & IPv6 static routing.
8	The Access Switch should support IPv6 management features like IPv6 ping, IPv6 trace route, IPv6 Telnet, IPv6 TACACS, IPv6 DNS, and IPv6 RADIUS.

7. Access Switch 24 Port POE

Sr. No.	Specifications
1	Access Switch should have 24 ports of 100/1000 PoE+(802.3 at) RJ45 and *minimum* 2 ports of 10G (2 SFP+ for uplink).
3	The Access switch should support min VLANs.
4	The Access Switch should support minimum stacking up to 4 units. Cost of the stacking modules/Ports should be included.
5	The Access Switches should support link aggregation across the stack.
6	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
7	The Access Switch should support full Layer 2 features like STP, RSTP, MSTP, LAG, LACP, ACL, QoS.
8	The Access Switch should support basic L3 features like IPv4 & IPv6 static routing.
9	The Access Switch should support IPv6 management features like IPv6 ping, IPv6 trace route, IPv6 Telnet, IPv6 TACACS, IPv6 DNS, and IPv6 RADIUS.
10	All the ports should be usable at full power.

8. Access Switch 48 Port

Sr. No.	Specifications
1	Access Switch should have 48 ports of 100/1000 RJ45 and *minimum* 2 ports of 10G (2 SFP+ for uplink).
2	The Access switch should support VLANs.
3	The Access Switch should support minimum stacking up to 4 units. Cost of the stacking modules/Ports should be included.
4	The Access Switches should support link aggregation across the stack.
5	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
6	The Access Switch should support full Layer 2 features like STP, RSTP, MSTP, LAG, LACP, ACL, QoS.
7	The Access Switch should support basic L2 features like IPv4 & IPv6 static routing.
8	The Access Switch should support IPv6 management features like IPv6 ping, IPv6 trace route, IPv6 Telnet, IPv6 TACACS, IPv6 DNS, and IPv6 RADIUS.

9. Access Switch 48 Port POE

Sr. No.	Specifications
1	Access Switch should have 48 ports of 100/1000 PoE+(802.3 at) RJ45 and *minimum* 2 ports of 10G (2 SFP+ for uplink).
2	The Access switch should support min VLANs.
3	The Access Switch should support minimum stacking up to 4 units. Cost of the stacking modules/Ports should be included.
4	• The Access Switches should support link aggregation across the stack.
5	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.

6	The Access Switch should support full Layer 2 features like STP, RSTP, MSTP, LAG, LACP, ACL, QoS.
7	The Access Switch should support basic L3 features like IPv4 & IPv6 static routing.
8	The Access Switch should support IPv6 management features like IPv6 ping, IPv6 trace route, IPv6 Telnet, IPv6 TACACS, IPv6 DNS, and IPv6 RADIUS.
9	All the ports should be usable at full power.

10. Indoor Wireless Access points

Vendor should provide atleast “very good” signal quality consistently at all points in the premises. A heat map of whole premises should also be provided without any blackholes after conducting a site survey.

S.No	**Specifications Indoor AP**
	Indoor Access Points 802.11a/b/g/n/ac Wave 2
1	Access Point radio should be minimum 4x4 MU- MIMO with 4 spatial streams on 5GHzand should also have 2.4GHz.
2	Access Point should be 802.11ac Wave 2.
3	AP should have 1 G PoE LAN port.
4	802.11 a/b/g/n/ac functionality certified by the Wi-Fi alliance.
5	Access Point can have integrated or external Antenna.
6	The Max transit power of the AP + Antenna should be as per WPC norms for indoor Access Points. OEM to give a undertaking letter stating that the AP will be configured as per WPC guidelines for indoor AP and also submit the WPC certificate showing approval.
7	Access point could have Internal/External Bluetooth Low energy beacon to support advance location based services for Mobile engagement solutions and applications.
8	Should support 8x BSSID per AP radio.

9	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.
10	Should support BPSK, QPSK, 16-QAM, 64-QAM and 256 QAM (256 QAM for 802.11ac only).
11	Access point should have console port or SSH/Telnet access. Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.
12	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.
13	Must operate as a sensor for wireless IPS
14	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services
15	The Access Point should have the technology to improve downlink performance to all mobile devices.
16	Access point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization
17	AP mounting kit should be with locking mechanism/ Kensington Lock so that AP cannot be removed without using special tools.
18	AP should be UL 2043 certified.
19	Must support Power over Ethernet, local power (DC Power), and power injectors.
20	802.11e and / or WMM
21	Must support QoS for voice and video etc.
22	Access Point should be 802.11 DFS certified
23	AP should be manageable with wireless access controller.

11. Outdoor Wireless Access Point

Sr. No	Description
	Outdoor Access Points 802.11a/b/g/n/ac Wave 2

1	Access Point radio should be minimum 4x4 MU- MIMO with 4 spatial streams on 5GHzand should also have 2.4GHz.
2	Access Point should be 802.11ac Wave 2 ready from day one
3	AP should have 1x10/100/1000 Ge LAN port.
4	802.11 a/b/g/n/ac functionality certified by the Wi-Fi alliance.
5	Access Point can have integrated or external Antenna.
6	The Max transmit power of the AP + Antenna should be as per WPC norms for outdoor Access Points. OEM to give a undertaking letter stating that the AP will be configured as per WPC guidelines for outdoor AP and also submit the WPC certificate showing approval.
7	Access point may have Internal/External Bluetooth Low energy beacon to support advanced location based services for Mobile engagement solutions and Applications.
8	Should support 8x BSSID per AP radio.
9	Access point should support 802.11ac beamforming for 802.11ac.
10	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.
11	Should support BPSK, QPSK, 16-QAM, 64-QAM and 256 QAM (256 QAM for 802.11ac only).
12	Access point should support 802.3af/at POE standard.
13	Access point should have option of external power adaptor as well.
14	Access point should have console port.
15	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.
16	Must operate as a sensor for wireless IPS.
17	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services.
18	The Access Point should have the technology to improve downlink performance

	to all mobile devices.
19	Access point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization
20	AP mounting kit should be with locking mechanism/ Kensington so that AP cannot be removed without using special tools.
22	AP should support standalone mode/ Inbuilt Virtual controller mode for specific requirements.
23	AP should be IP66/67 certified.
24	AP should support -10 to +55 Degree operating temperature.

12. Wireless Controller & Security Solution

Security and Advanced WIDS/WIPS Features may be either integrated with controller or separate. (If separate then both should be of same OEM)

S.no	Specifications
	Hardware Specifications
1	Each WLAN Controller should support minimum of 1500 Access points. If any bidder can’t provide WLAN controller to support 1500 AP in single RU form factor, multiple controllers, controllable through single master console, must be proposed to meet the requirement. The proposed controller should support N+N redundancy.
2	Should have atleast 2 x 10 Gigabit Ethernet interface.
3	Controller should have required console port and USB ports.
4	Controller should have internal hot swappable redundant power supply.
5	Controller should have capacity to handle minimum 20000 or more concurrent devices.
6	The controller should support 802.11ac standard.
	Wireless Controller Features
7	The Controller must support an ability to dynamically adjust channel and power settings based on the RF environment.

8	The Controller RF management algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference. Quoted Access point must support necessary spectrum analysis functionality to achieve this.
9	The Controller must support interference detection and avoidance for both Wi-Fi and non-Wi-Fi interference.
10	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.
11	The controller should support advance QOS to implement role based access for data, voice and video applications. It should support session prioritization as well like Voice, Video, should get different QoS.
12	Support profiling of wireless devices based on known protocols like http and dhcp to identify clients
13	Should support visibility and control based on the type of applications
14	The controller should provide differentiated access for Guests and valid user groups. Guests should have restricted access (without telnet & SSH services). Similarly other ROLE BASED ACCESS policy support should be available for differentiated access.
15	The controller should provide latest network authentication (WEP, WPA, WPA2) and encryption types like TKIP and AES.
16	Controller should support reliable fast roaming standards 802.11k/r
17	Controller should support management frame protection.
18	The Controller Should provide a dashboard of spectrum quality in terms of the performance and impact of interference on the wireless network identifying the problem areas and channel utilization. Quoted Access Point should support this feature to send necessary data to controller.
19	The Controller should provide a spectrum Quality detail on a per- radio basis to help gauge the impact of interference on the network. Quoted Access Point should support this feature to send necessary data to controller.
	Security and Advance WIDS/WIPS Features
20	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.

21	Should support port-based and SSID-based IEEE 802.1X authentication.
22	Should support MAC authentication to provide simple authentication based on a user's MAC address.
23	WLC Should support Rogue AP detection, classification and standard WIPS signatures.
24	WLC should be able to exclude clients based on excessive/multiple authentication failure.
26	WIPS solution should Automatically blacklist clients when it attempts any attack.
27	WIPS solution should be capable of wireless intrusion detection &prevention . The WLAN should be able to detect Rogue AP and take corrective action to prevent the rogue AP. The system should detect and prevent an organization’s wireless client connecting to rogue AP and also prevent an outside client trying to connect to organizational WLAN.
28	WIPS solution should detect & prevent an Ad-hoc connection (i.e. clients forming a network amongst themselves without an AP) as well as windows bridge (client that is associated to AP is also connected to wired network and enabled bridging between two interfaces)
29	The system should detect an invalid AP broadcasting valid SSID and should prevent valid clients getting connected from these AP’s.
30	WIPS Solution should track the location of interferer objects.
31	For advance forensic WIPS solution should perform spectrum analysis to detect and classify sources of interferences. System should provide chart displays and spectrograms for real-time troubleshooting and visualization.
32	The WIPS solution should be able to detect and locate the rogue access point on floor maps once detected with NMS.
33	The WIPS solution should be able to detect and prevent if a client uses FATA-Jack 802.11 DoS tool (Available free on internet) and tries to disconnect other stations using spoofed authentication frames that contain an invalid authentication algorithm number.
34	The WIPS solution should detect and protect if a client probe-request frame will be answered by a probe response containing a null SSID to crash or lock up the firmware of any 802.11 NIC.

35	The WIPS solution should detect and protect if a client/tool tries to flood an AP with 802.11 management frames like authenticate/associate frames which are designed to fill up the association table of an AP.
36	The WIPS solution should detect and protect if a client/tool keeps on sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF) to disconnect all stations on a network for a widespread DoS.
37	The WIPS solution should detect and protect if somebody tries to spoof mac address of client or AP for unauthorized authentication.
38	The WIPS solution should detect and protect if a client/tool tries de-authentication broadcast attempts to disconnect all clients in range rather than sending a spoofed de-authentication to a specific MAC address.
39	The WIPS solution should detect and protect if an attacker attempts to lure a client to a malicious AP using SSID on fake AP in close proximity of the premises. It should detect When the Valid Client probes for Valid SSID and these malicious APs respond and invite the client to connect to them.
40	When client radio is in sleep mode to save battery and AP then begins buffering traffic bound for that client until it indicates that it is awake. The WIPS solution should detect and protect if intruder tries sending spoofed frames to the AP on behalf of the original client to trick the AP into believing the client is asleep to buffer the AP beyond limit.

13. NETWORK MONITORING SYSTEM (NMS)

NETWORK MONITORING SYSTEM (NMS)	
Sr. no.	**Specifications**
1	The complete Network Management Solution (hardware and software etc.) providing secured web-based consoles to monitor devices as per BOQ, including servers and Applications. It should have scalability to manage up to 2500 devices approx. with support for SNMP v1-3, IPV4 & IPV6. It should be certified to run on Linux/CentOS/RHEL/Ubuntu/Other Linux.
2	The Network Management Software should provide a customizable at-a-glance summary of all discovered devices, including inventory and event summary information used to proactively identify problem areas and help prevent network downtime.

3	The Network Management Software should be able to discover layer3 & layer 2 heterogeneous environment and configure, monitor, manage, and deploy configurations to dynamically update groups of devices including virtual servers.
4	The Network Management Software should allow flexible definitions of administrator roles and responsibilities with RBAC (Role based Access Control) for different teams.
5	The Network Management Software should provide an interface to configure and deploy Command Line Interface (CLI) based configuration templates across one or more IP devices.
6	The Network Management Software should enable performance management by providing customizable dashboard(s).
7	The Network Management Software should be able to generate reports designed to summarize utilization of and traffic patterns on network interfaces.
8	The Network Management Software should be able to provide real-time network monitoring and accounting capabilities without impacting network performance.
9	The Network Management Software should allow administrators to track device configuration changes, enabling viewing, retrieval, and restoration of configuration files, and monitoring of configuration for troubleshooting purposes.
10	Solution must provide Wireless LAN Planning and Design, Network Monitoring and Troubleshooting, Indoor location monitoring capability, Centralized Software updates, Network mapping with floor plans for easier automated site survey.
11	Display the location of each rogue device on a building floor plan.
12	System should provide current list of clients connected to each AP, graphical details of wireless traffic & data rates on a per client basis, recent history of association with APs &adhoc networks for clients, alerts when wireless clients use interface bridging or Internet.
13	System should provide DNS response times for every user. Aggregated DNS response information per server.
14	System should provide client troubleshooting information including Association time.
15	Connection Sharing, trends for WLAN performance parameters, alert when wireless bandwidth is being wasted due to excessive auxiliary traffic, trends for WLAN performance parameters

16	System must be able to maintain recent history of connected clients for each AP for up to 2 years. Archieve of logs.
17	The operations solution should provide a network “dashboard” on screens, providing up-to-date network-wide information on key usage and performance metrics.The operations solution should monitor all network devices including edge switches to which wireless devices are connected.

14. FIREWALL

Sr. No.	Firewall
1	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems
2	The Proposed Firewall Vendor should be in the Leaders Quadrant of Gartner Magic Quadrant for NGFW.
3	Firewall appliance should have at least 16 x 1GE interfaces, 8 x 1GE SFP interfaces 4 x 10G SFP+ interfaces
4	Firewall Throughput should be 50 Gbps
5	Firewall should support minimum 20 Gbps of VPN throughput
6	Firewall should support 2000 site-to-site & client to site VPN Tunnels
7	Firewall should support minimum 2,000 concurrent SSL VPN users and should be scalable in future
	Firewall should support minimum 2500 concurrent users and should be scalable in future
8	Firewall should support 200,000 new sessions per second
9	Firewall should support 10 Million concurrent sessions
10	The solution should support minimum 7 Gbps of NGFW (FW + IPS + AVC) throughput for Mix / production traffic
11	The solution should support minimum 4.5 Gbps of Threat Prevention (FW + IPS + AVC + AV) throughput for Mix / production traffic

12	The Firewall solution should support NAT64, DNS64 & DHCPv6
13	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.
14	The proposed system should have integrated Traffic Shaping functionality.
15	The Firewall & IPSEC VPN module shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification.
16	The proposed system should support
	a) IPSEC VPN
	b) PPTP VPN
	c) L2TP VPN
17	The device shall utilize inbuilt hardware VPN acceleration:
	a) IPSEC (DES, 3DES, AES) encryption/decryption
	b) SSL encryption/decryption
18	The system shall support the following IPSEC VPN capabilities:
	a) Multi-zone VPN supports.
	b) IPSec, ESP security.
	c) Supports NAT traversal
	d) Supports Hub and Spoke architecture
	e) Supports Redundant gateway architecture
19	The system shall support 2 forms of site-to-site VPN configurations:
	a) Route based IPSec tunnel
	b) Policy based IPSec tunnel
20	The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode.
21	The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in

	an IPSec VPN.
	Virtualization
22	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 5 Virtual Firewall license should be provided.
	Intrusion Prevention System
23	The IPS capability shall minimally attain NSS Certification
24	IPS throughput should be minimum 12 Gbps for Mix / Production traffic
25	The IPS detection methodologies shall consist of:
	a) Signature based detection using real time updated database
	b) Anomaly based detection that is based on thresholds
26	The IPS system shall have at least 7,000 signatures
27	IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available
28	In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved
29	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.
30	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident
31	Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
	Antivirus
32	Firewall should have integrated Gateway Antivirus solution

33	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:
	a) HTTP, HTTPS
	b) SMTP, SMTPS
	c) POP3, POP3S
	d) IMAP, IMAPS
	e) FTP, FTPS
34	The proposed system should be able to block or allow oversize files based on configurable thresholds for each protocol types and per firewall policy.
	Web Content Filtering
35	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.
36	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
37	The proposed system shall provide web content filtering features:
	a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.
	b) Shall include Web URL block
	c) Shall include score based web keyword block
	d) Shall include Web Exempt List
38	The proposed system shall be able to query a real time database of over 110 million + rated websites categorized into 70+ unique content categories.
	Application Control
39	The proposed system shall have the ability to detect, log and take action against network traffic based on over 2000 application signatures
40	The application signatures shall be manual or automatically updated

41	The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions
	Data Leakage Prevention
42	The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.
	High Availability
43	The proposed system shall have built-in high availability (HA) features including associated accessories, cables etc.
44	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.
45	High Availability Configurations should support Active-Active and Active-Passive.
	Logs and Reports
46	Should have atleast 500 GB of Hard Drive Capacity for logging and reporting.
	It should automatically transfer the archives of the logs to a NAS.
47	Real-time display of information to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP/HTTPS traffic.
	Management
48	Management solution (virtual appliance) for all the appliances shall be provided
49	Should be configurable using CLI, GUI interface and central management software. Should support SNMP, SSH, Telnet, HTTP(s)
50	The management system must be capable of pushing NGFW security policies and configurations to individual or multiple NGFWs through secure, encrypted connection interfaces.
51	Supports role-based administration of NGFW
	License
52	5 Years 24x7 support and license for Gateway Antivirus, IPS, IDS, Web filter,

	Anti-Spam, application filtering, botnet, DLP and hardware support License.

15. Server Hardware (for NMS and DHCP and other virtual appliances)

Sr. No.	Item	Description
1	**Server Form Factor**	Rack mount
2	**Processor type**	Intel Xeon 64 bit Processor E5 6000 series v4 or Xeon Scalable Processor (12-core /16MB Cache min) or equivalent AMD Epyc Processor
3	**Number of processors**	2 Processor or superior
4	**Standard memory**	256 GB
5	**Internal hard disk drive**	Minimum 5 nos. 1.2TB 6G SAS 10k or higher, Hot swappable PLUS Minimum 2 nos. 200 GB SATA / NVME SSD, Hot swappable Support for minimum 12 SFF/LFF SAS drives
6	**Hard disk controller**	Smart Array P420 /1GB FBWC Controller or equivalent or higher Support hardware RAID in 0/1/5/6/10/5plus spare configurations. Battery for power loss protection included Adequate number of cards to support all the 12 HDD bays should be provided from day one
9	**Power Supply**	Redundant N+N Hot Pluggable power supply
10	**Network interface**	At least Two Nos. Embedded Dual Port 10G SFP+ NIC
	Cooling Fans	N+N hot pluggable. Should be able to maintain temperature range XXXXXXXXX
11	**Management**	IP based HTTP/HTTPS Management capability on atleast 1G network interface
13	**Operating system Compatibility**	Certified for Windows , RHEL/CentOS/Ubuntu/Fedora/Debian, VMWare

14	**Accessories**	All rails, cables, cords etc needed for installation of server in standard rack should be included
15	**Software**	VMWare license for two processors included

16. Network Access Control (NAC): for 10000 concurrent devices/endpoints.

Complete NAC solution: open source (openNAC, or Packet Fence Preferred) or COTS , including Hardware in N+N, for its implementation at the enterprise wide heterogeneous network of AIIMS, New Delhi and for NCI , Jhajjar.

The solution must include configuration, customization, integration, implementation and support. Should have the approach that combines AAA, NAC, BYOD and Guest Access by incorporating identity, health, physical/device information, and conditional elements into one set of policies. It should be certified to run on Linux/CentOS/RHEL/Ubuntu/Other Linux.

S No.	**Functionality**
1	Web-based interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.
2	Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).
3	Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures (endpoint health).
4	Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.
5	If a license is required to provide profiling functionality, it should be included and be perpetual.
6	AAA server must support both functionality: RADIUS server for client device authentication and TACACS+ for network device authentication and logging from day 1. Overlay component can be added to achieve both functionalities.
7	All external facing interfaces should be programmable, which means APIs should be available to extend the system to support different authentication protocols, identity stores, health evaluation engines, and port and vulnerability scanning engines.

8	The solution must be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:
	• Built-in guest management and device/user onboarding
	• Web based management interface with dashboard
	• Reporting and analysis with custom data filters
	• Data repository for user, device, transaction information
	• Rich policies using identity, device, health, or conditional elements
	• Deployment and implementation tools.
9	AAA framework must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against an external SQL database.
10	Authentication or authorization support for LDAP, AD, Kerberos, Token Server, SQL compliant database
11	Should support multiple methods for device identification and profiling such as:
12	Integrated, network based, device profiler utilizing collection via SNMP, DHCP, HTTP, AD, ActiveSync
13	Endpoint audit via NESSUS or NMAP scanning
14	Policy creation tools:
	• Pre-configured templates
	• Wizard based interface
	• LDAP browser for quick look-up of AD attributes
	• Policy simulation engine for testing policy integrity
15	Policy model should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.
16	Support the following enforcement methods:
17	VLAN steering via RADIUS IETF attributes and VSAs

18	VLAN steering and port bouncing via SNMP
19	Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs.
20	Roles or any other vendor-specific RADIUS attribute supported by the network device.
21	Agent-based enforcement – bouncing a managed interface and sending custom messages. Also, control access to different networks via whitelist and blacklist. License should be included.
22	Must be able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication.
23	Must support complex PKI deployment where TLS authentication requires validating client certificate from multiple CA trust chain. Must also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.
24	**Reliability / Performance**
25	Appliances have ability to be clustered in any combination via local and remote network connections providing unlimited scale, redundancy, and load balancing.
26	Platform must be deployable in an out-of-band model and support clustering .
27	Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.
28	Must support several deployment modes including centralized, distributed, or mixed.
29	**BYOD**
30	Should support self-service workflow for smart devices as well as traditional computing platforms
31	Unique portal pages based on devices type – iOS, Android. Etc.
32	Ability to support revocation of devices.
33	Correlation of user, device, and authentication information for easier troubleshooting, tracking etc. – provides high level of visibility into what devices are on the network and associated with what users.

34	Automated onboarding of devices to enable secure access via self-serve portal allowing for the configuration of 802.1x supplicants, device enrolment and provisioning.
35	Ability to integrate with Active Directory / LDAP / KRB5 so users that are approved for BYOD may be authenticated via identity and/or device attributes.
36	BYOD solution should manage the individual device credentials in a partitioned database and not pollute the existing PKI with client certificates for BYO devices.
37	**Guest Access**
38	Solution must be capable of providing sponsored and self-provisioned Guest Access. License for minimum 1000 concurrent Devices / Users.
39	Ability to provide free and billable Guest Access with built in payment solution that can integrate with payment solution providers.
40	Must be able to provide custom branding.
41	Ability to send automated OTP SMS or email credentials to the Guest User.
42	Ability to set Account Details including Time Frame, Bandwidth Contract etc. Once account timeframe expires the User Account becomes inactive automatically.
43	Solution must be capable of providing Advertising Services (Play Video before Access, offer current Promotions, Advise of Health Alerts)
44	Guest solution should manage the individual guest credentials in a partitioned database and not pollute the user store with account credentials for guest users.
45	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
46	Access token login support for single credential login to guest network – event management, scratch cards etc.
47	Bulk import of guest accounts with ability to trigger notification of credentials via email.
48	Sponsored approval workflow for guest self-registration where open SSID registration can be protected by requiring internal staff to approve the creation of

	guest account.
49	Support URL persistence so users originally requested webpage can be displayed post login.
50	Published API's to allow 3rd party system to manage guest accounts.

17. Intelligent integrated/inbuilt infrastructure Rack for network infrastructure: Smart Rack Type 1

Specifications	
1	**a)** The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to TIA 942 guidelines thus shall be composed of multiple active power and cooling distribution paths, but only one path active. Shall have redundant components. **b)** The Intelligent Integrated Infrastructure essentially includes internal redundant or backup power supplies, environmental controls (e.g., precision air conditioning, fire suppression, smoke detection, Water leak detection, humidity sensor etc.), security devices etc. Critical systems like UPS and Precision Air-conditioning system will have N+N topology respectively.
2	Integrated and contained Cabinet: 42U rack of 2200 mm maximum height with min 30U of usable space.
3	Integrated and Redundant Precision Cooling Systems Suitable for 2x6 kW IT load with variable Scroll Technology (N+N redundancy)
4	2 x 10 KVA rack mount UPS with P.F. up to 0.9 & efficiency 92% ~94%. 12 Volt SMF batteries with backup of 10 minutes. UPS should be mounted inside the integrated rack and batteries would be kept external.
5	Thermal Containment
6	Rack should have integrated Fire Detection system.
7	Rack should have integrated “Novec 1230” gas suppression system
8	The Rack should have Monitoring capability over IP with required system(SNMP and HTTP/Web-management capability)
9	Integrated Rack should have Biometric Access Control - IP based Access Control

	System shall be used to serve the objective of allowing access to authorized.
10	Air conditioning modules should be controlled by microprocessor based controller. It can be programmed to control the function of every device within the unit via I/O. The controller allows setting and monitoring of the room parameters. Unit utilizes multiple temperature sensors placed at the rack inlet, to ensure management and control of temperature by rack. Each unit should be connected up to 10 Sensors.
11	The integrated monitoring system should allow monitoring of parameters like temperature, humidity, Fire alarm, rack sensor failure, smoke detection and other relevant parameters etc and also capable to send email alerts.
12	Humidifier is removable from the rear of the cabinet.
13	Cooling unit should have integrated heater and de-humidifier.
14	Rack should have Integrated rodent repellent system.
15	In case of cooling unit failure front door should automatically opened and exhaust system should start forced hot air removal.
16	32 Amp single phase PDU with 12- IEC C13 and 4-IEC C19 each rack should have two such PDUs.
17	Integrated rack should be supplied with inbuilt electrical distribution system.
18	Integrated Data centre/Server room infrastructure should be supplied with 5 years of warranty including batteries.
	Cable manager included
19	There should be a single window/OEM for services and maintenance for integrated rack.

18. Intelligent integrated/inbuilt infrastructure Rack for network infrastructure: Smart Rack Type 2

Specifications	
1	**a)** The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to TIA 942 guidelines thus shall be composed of multiple active power and cooling distribution paths, but only one path active. Shall have redundant components.

	b) The Intelligent Integrated Infrastructure essentially includes internal redundant or backup power supplies, environmental controls (e.g., precision air conditioning, fire suppression, smoke detection, Water leak detection, humidity sensor etc.), security devices etc. Critical systems like UPS and Precision Air-conditioning system will have N+N topology respectively.
2	Integrated and contained Cabinet: 24U rack of 2200 mm maximum height with min 15U of usable space.
3	Integrated Cooling Systems Suitable for 1 kW IT load with variable Scroll Technology
4	3 KVA rack mount UPS 12 Volt SMF batteries with backup of 10 minutes. UPS should be mounted inside the integrated rack
6	Rack should have integrated Fire Detection system.
8	The Rack should have Monitoring capability
16	32 Amp single phase PDU with 12- IEC C13 and 4-IEC C19
17	Integrated rack should be supplied with inbuilt electrical distribution system.
	Cable manager included
18	Supplied with 5 years of warranty including batteries.
19	There should be a single window/OEM for services and maintenance for integrated rack.

19. Server Room Specification

S. No.	**Server Room Infrastructure**
1	**Raise floor system:** Providing of Raised flooring (Up to 300 mm height) : The Access Floor System shall comprise 600mm x 600mm Laminated square panels, Uniform Distributed *Load(*UDL) -1350 kg with point load 450 Kg.
2	Lifting devices: Providing of panel lifting suction devices for lifting the floor pane
3	**Fire Rated Gypsum Panelling**: Gyp board to be faced inner sides of server Room with 12 mm thick fire line gypsum board and Ceiling Area Partition shall be finished with jointing tape / compound etc.

4	Preparing of wall for painting includes making smooth surface with wall putty and Termite Spray.
5	Applying emulsion water-based, 100% acrylic, interior paint, on ceiling walls three coats with roller including applying cement primer.
6	Double Glazing of partitions and windows.
7	Dust proof and leak proof gasket sealed doors / windows.
	Fire Alarm system
1	2 zone fire alarm Panel.
2	Smoke Detector
3	Manual call point
4	Sounder
5	Supply of 1.5 X 2 core copper cable for FAS.
6	Clean Agent Gas based wall mount FIRE EXTINGUISHER (4 KG)
	Electrical Work/UPS/AC
1	Cable Tray 200 X 40 mm Electrical Fabricating supplying to site of installation on floor/ surface , height 40 mm. including providing all fixing accessories as required.
2	UPS power supply Point from 2 Different Sources
3	Fixing of Precision AC: 2 ton each X 4 nos.
4 5	Proper Earth Point need to provide to connect the server racks & Electrical equipment. **4 way UPS DB with Incomer**
6	63A 4P MCB--- 1 No,
7	32A 2P MCB--- 6 Nos (Outgoings)
8	32 AMP X 1ph 3 pin Industrial plug and Socket For Server Racks
9	Wiring for UPS Power of Server Racks points with three core, 6.0 sqmm FR PVC Insulated and PVC sheathed flexible cable with bright annealed electrolytic copper conductor.

	SECURITY and MANAGEMENT
1	Biometric access control system
2	Water leakage detection system
3	Rodent detection system
	Data centre shall be developed as per the industry standard. Temperature in the data centre should be maintained between 15^{o}C to 20^{o}C. All necessary arrangements shall be made by IT agency to comply this during the warranty period of 5 years/ CAMC period of 5 years. In addition to the above, any other item/hardware/software/cable accessories etc. is to be supplied and installed by the IT agency as per the requirement of the site for completeness of the data centre. Data Centre should be capable and scalable to cater the future requirements like installation of all the servers etc. NOTE- It is under the scope of IT agency to run the Data Centre (s) 24x7 smoothly during the maintenance period. Any item related with electrical, HVAC, civil etc. is to be provided by the IT agency during the warranty period of 5 years/ CAMC period of 5 years.

CABLING FOR DATA SYSTEM

1. All Passive components (Copper and Fibre) must be from the same OEM.
2. For CAT 6 A cables including patch cords must be – each individual pair separately shielded.
3. Insulation must be fire retardant.
4. All CAT 6 A and Fibre cables must be LSZH.
5. The OEM shall be ISO 9001:2000certified
6. The OEM shall be ISO 14001accredited
7. The Copper and Fiber cabling system shall be certified by OEM to have application support warranty for 25years

COPPER CABLING SYSTEM

<u>1.1 CAT6A Foiled Twisted Pair Cable</u>	
Characteristic	**Min. Required Specification**
General Features	Category 6A must be solid copper conductor 23 AWG having NVP: 75-77% with 4 pair individually foiled LSZH cable and must be compliant with TIA/EIA-568-C.2/ 3P for 500MHz (ETL certificate to be enclosed along with the bid.
<u>1.2 FACE PLATE: 1 port or two port</u>	
Characteristic	**Min. Required Specification**
Features	Single/Double Gang as per the requirement & complete in all respect and as directed to the satisfaction of engineer
	Labeling provision must be there.
Characteristic	**Min. Required Specification**
1.3 CAT6A SHIELDED RJ45 JACK	
Features	Must be compliant with latest ISO/IEC 11801 A1.1 draft and ratified TIA/EIA 568-C.2/ 3P for the support of 10GBASE-T.
	Must use insulation displacement connectors (IDC)
	Allow for a minimum of 50 re-terminations without signal degradation.

	Be constructed of high impact, flame-retardant thermoplastic and robust die cast zinc alloy housing with icon options for better visual identification.
	With shutter provision to protect from dust and moisture. If shutter provision is not available on RJ45 jack it is acceptable on face plate also.
	It should follow 568A/B wire patterns/configuration
	Color options in jacks should be available.
	The I/O should be UL/ third party certified (Authorized of govt. agencies).
Mechanical Characteristic: Jack Connector	**Plastic Housing:** Robust die cast Zinc Alloy housing plated with Bright Nickel/Cu
	Operating Life: Minimum 750 insertion cycles
	Contact Material: Copper alloy / Gold-Plated Bronze
	Contact Plating: >0.75 micrometers Gold/Ni
Characteristic	**Min. Required Specification**
1.4 CAT 6A 24 PORT JACK / patch PANEL LOADED	
Features	Be made of steel/aluminum, in 24 port configurations. Each jack for the jack panel should have shuttered or dust cover with jack for dust free environment.
	Have port identification numbers on the front of the panel.
	Should have self-adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel, with optional color labels / icons.
	Each port / jack on the panel should be individually removable on field from the panel.
	Should be certified by third Party like UL. Certificates to be submitted with bid.
	Should be supplied with metallic rear cable management shelf/support bar as a part of Jack Panel.

1.5 CAT 6A SHIELDED PATCH/MOUNTING CORDS (1 Mtr., 2 Mtr. and 3 Mtr.)	
Characteristic	**Min. Required Specification**
Features	Category 6A Equipment cords (Length – 1mtr and 3mtr.)
	The work area equipment cords shall be comply with TIA/EIA-568- C.2/3P Performance Specifications for 4 pair Category 6A Cabling.
	Category 6A equipment cords: Shall be round, and consist of eight insulated 26 AWG, stranded bare copper conductors, arranged in four color-coded twisted-pairs each pair should be foiled with aluminum shield.
	Equipped with 8-position shielded plugs on both ends, wired straight through with standards compliant wiring.
	Should have 50 micro inches of gold plating over nickel contacts.
	Modular cords should include a molded strain relief boot.
	Should be certified by UL/ third party.
MechanicalCharacteristic: patch cord Cable	**Conductor size:** 26 AWG stranded bare copper.
MechanicalCharacteristic: Plug	**Jacket:** LSZH
	Temperature range: -10°C to +60°C
	Operating life: Minimum 750 insertion cycles
	Contact Material: Copper alloy/Gold-plated bronze
	Contact plating: >0.75 micrometers Au/Ni

2.0 OPTICAL FIBER CABLING:

2.1 24 Core Single-Mode(SM) 9/125 µm OS2 Armoured Multi-Tube Optical Fiber Cable 6 cores, 12 cores and 24 cores:-	
Characteristic	**Min. Required Specification**
Features	The fiber type should be 9/125 **µm**, OS2 Matched Cladding Single Mode optical fiber.

	Fiber should be coated with acrylate coating.	
	The fiber should be optimized for operation at 1310 nm and at 1550 nm.	
	Should fulfill the requirements of ISO.IEC 11801 - 2nd Edition, type OS2, ITU-T REC G 652D specification.	
Physical Characteristics:-	No of Cores	6 core, 12 cores and 24 cores
	Nominal mode field diameter	9 µm
	Mode field diameter tolerance	±0.5µm
	Cladding diameter	125 µm
	Cladding diameter tolerance	±1.0 µm
Optical Characteristics:-	**Attenuation (of cable with fibers):**	
	At 1310 nm	≤ 0.35 dB/km
	At 1550 nm	≤ 0.22 dB/km
	Polarisation Mode Dispersion (PMD)	≤ 0.06(ps/sq km)
	Proof Stress level	> 0.7 (~ 1%) GPa
	Core-Cladding Concentricity error	≤ 0.5µm
	Cladding non-circularity	≤ 0.7 %
	Diameter of outer coating layer	242 ± 5 µm
	Cut-off wavelength	≤ 1260 nm
Construction Details:-	CORE	Germanium doped core with no phosphorus i.e. reduced tendency for hydrogen degradation.
	COATING	UV-curable dual layer acryl ate coating, which ensures excellent micro bending and abrasion resistance.
	Fibre/Tube Identification	Color coded
	Fibre protection(Tubes)	Polybutylene Terephthalate (PBT)
	Armor	Corrugated Steel tape Armor (ECCS Tape)

	Inner Jacket	High density polyethylene
	Outer Jacket	UV Stabilized High density polyethylene (HDPE) LSZH.
	Outer Jacket Color	Black
	Central Strength Member	Fibre Reinforced Plastic(FRP)
Dimensions:-	Cable Diameter	15.1 ± 4.0 mm
Mechanicaland Environmental	Max Bend Radius(full load)	10 X Overall diameter
	Max. Bending Radius (during installation)	20 X Overall diameter
Performance:-		
	Max. Tensile Strength-Short Term	Minimum 2000N
	Max. Crush Resistance-Short Term	Minimum 4000N/10 cm
	Operating Temperature range	-10°C to +70°C

2.2 12 CORE Multi-Mode 50/125 µm OM4 Armoured Multi-Tube Optical Fiber Cable 6 cores and 12 cores:-

Characteristic	**Min. Required Specification**	
Features	The fiber type should be 50 / 125, OM4 Graded Index Fiber cable	
	Fiber shall be coated with acrylate coating.	
	The fiber should be optimized for operation at 850 nm and at 1300 nm.	
	Should fulfill the requirements of ISO/IEC 11801:2002- 2nd Edition, Type OM4;	
Physical Characteristics:-	No of Cores	6 cores and 12 cores
	Nominal mode field diameter	50 µm
	Mode field diameter tolerance	±2.5µm
	Cladding diameter	125 µm

	Cladding diameter tolerance	±2.0 µm
Optical Characteristics:-	**Attenuation (of cable with fibers):**	
	At 850 nm	<=2.7dB/km
	At 1300 nm	<= 0.8 dB/km
	Bandwidth:	
	At 850 nm	>= 2000 MHz · km
	At 1300 nm	>= 500 MHz · km
	Numerical aperture	0.200 ± 0.015
	Diameter of outer coating layer	245 µm (without coloring layer)
	Tolerance of coating layer diameter	±10 µm
Construction Details:-	CORE	Germanium doped core with no phosphorus i.e. reduced tendency for hydrogen degradation.
	COATING	UV-curable dual layer acryl ate coating, which ensures excellent micro bending and abrasion resistance.
	Fibre/Tube Identification	Color coded
	Fibre protection(Tubes)	Polybutylene Terephthalate (PBT)
	Armor	Corrugated Steel tape Armor (ECCS Tape) Thickness.
	Inner Jacket	High density polyethylene
	Outer Jacket	UV Stabilized High density polyethylene (HDPE) LSZH.
	Outer Jacket Color	Black
	Central Strength Member	Fibre Reinforced Plastic(FRP)
Dimensions:	Cable Diameter	15.1 ± 4.0 mm
Mechanical and	Max Bend Radius(full load)	10 X Overall diameter

Environmental Performance:-	Max. Bending Radius (during installation)	20 X Overall diameter
	Max. Tensile Strength-Short Term	Min 2000N
	Max. Crush Resistance-Short Term	Min 4000N/10 cm
	Operating Temperature range	-10°C to +70°C

2.3 Fiber Optic LIU:-

Fiber optic patch panel	Fibre management enclosures that can be used as a wall mount enclosure for isolated applications or rack mount enclosure for integrated applications.
Height	1 U, 1.75 inches
No. of fiber ports	12/24
Material	Powder coated Mild Steel/aluminum
	Rugged steel/aluminum construction in graphite finish
	Rear, side & base access for Incoming / Outgoing fiber cables
Cable Management rings	Management rings within the system to accommodate excess fibre cordage behind the through adapters and maintain fibre bend radius.
Adaptor Slots	Built in Slots for LC adaptors.
Sliding cover	Panel cover is of slide out for easy operation & maintenance
Splice Tray	24Fiber Splice Tray of ABS material should be supplied for the LIU.

2.4 Fiber Optic Adaptors (Single mode):-

Fiber optic adaptors	LC Type Single Mode Adaptors
Type	LC Type
	Meets TIA/EIA 568-C.3 and IEC 874-109 standards
	Adapters should be snap mount for easy insertion and removal.

	Shuttered feature protects from light emissions and dust.
Material Ferrule	Zirconia Alignment sleeve
2.5 Fiber Optic Pigtail 9/125 Singlemode OS2 LC Type:-	
Fiber optic pigtails	**Single mode OS2 Pigtails with LC connector**
Type	9/125 micron OS2fibre performance
Cordage Outer Diameter:	2.0mm ±0.1mm x 4.1 ± 0.2mm
Cable	900µmTight Buffered
Retention Strength	100N
Jacket Material	LSZH
Operating Temp.	-10ºC to 75ºC
Connector Insertion Loss	0.30dB(Max)
2.6 Fiber Optic Patch Cord LC-LC 9/125 OS2 Singlemode:-	
Fiber Optic Patch Cords	**LC-LC 9/125 µm, OS2 Singlemode Duplex Patch Cord**
Cable	9/125 µm, OS2 SM, Duplex patch cord.
Connectors	The optical fiber patch leads shall comprise of Single-mode 9/125µm OS2 fiber with 2x LC type fiber connectors terminated at both end of the patch cord.
Cordage O.D	(Duplex): 2.0mm ± 0.1mm x 4.1± 0.2mm
Cable	900µmTight Buffered
Strength Member	Aramid Yarn
Jacket Material	LSZH

Connector Loss	0.30dB(max)
Operating Temperature	-10°C to +70°C
*For 100G connectivity for distance of 2KM Required trans-receivers, patch cords etc.	
2. 7 Fiber Optic Adaptors (Multimode):-	
Fiber optic adaptors	LC Type Multimode Adaptors
Type	LC Type
	Meets TIA/EIA 568-B.3 and IEC 874-109 standards
	Adapters should be snap mount for easy insertion and removal.
	Shuttered feature protects from light emissions and dust
Material Ferrule	Zirconia Alignment sleeve
Insertion Loss	<0.34dB Max
Operating Temperature	-10°C to +70°C
2. 8 Fiber Optic Pigtail 50/125 Multimode OM4 LC Type:-	
Fiber optic pigtails	**Multimode OM4 Pigtails with LC connector**
Type	50/125 micron OM4 fibre performance
CordageOuter Diameter:	2.0mm ±0.1mm x 4.1 ± 0.2mm
Buffer Diameter:	900µm
Primary Coating :	245µm
Jacket Material:	LSZH
Operating Temp.	-10°C to +60°C

Connector Insertion Loss	0.30dB(Max)

2. 9 Fiber Optic Patch Cord LC-LC 50/125 OM4 Multimode:-

Fiber Optic Patch Cords	**LC-LC 50/125 µm, OM4 Multimode Duplex Patch Cord**
Cable	50/125 µm, OM4 MM, Duplex Zipcord.
Connectors	The optical fiber patch leads shall comprise of Multi-mode 50/125µm OM3 fiber with 2xLC type fiber connectors terminated at both ends of the patch cord.
Cordage O.D	(Duplex): 2.0mm ± 0.1mm x 4.1± 0.2mm
Buffer Diameter	900µ tight buffer
Strength Member	Aramid Yarn
Jacket Material	LSZH
Connector Loss	0.30dB(max)
Operating Temperature	-10°C to +70°C

2.10 Gang Box (As per approved make)

Gang Box	Surface mounted , Plastic/ PVC Material, White Colour, supports one or two I/O ports

2.11 Cat 6 Unshielded RJ45 Connectors (As per approved make)

RJ45 unshielded Connector	Standard Acrylic unshielded RJ45 connector

Annexure-D

Technical compliance of items IT components (LAN & Wi-Fi) (Add one more column in the last as remarks and another column before tech specs for parameter)

Sr. no.	Technical Specification	Comply (Yes/No)	Page	Parameter	Remarks
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Annexure-E

List of approved makes for IT Work

Sr. No.	ITEM	MAKE
1.	Core Switch/ Distribution Switch/Access Switch	HP/Cisco/Juniper/Brocade/Extreme/ DELL/Mellanox/Fortinet
3.	Network Management Solution	HP/Cisco/Juniper/Brocade/Extreme/ DELL/Mellanox
4.	Wireless Solution (Wireless Access Point and Wireless Controller)	Aruba/Ruckus/Cisco/Juniper/Brocade/ Extreme /DELL/Mellanox
5.	Firewall	Cyberoam/Fortinet/Sophos/Cisco/ Juniper/Checkpoint/ Palo Alto
6.	Passive Components (Passive devices for LAN)- Cat 6A, Wall Plate 1 Port/2 Port, Power Cat6A Jack, Cat 6A Patch Cord, GANG Box, 24 Port Patch Panel CAT-6A etc.	Molex / Systimax / Panduit / D-Link / AMP/ R&M
7.	Optical Fibre Cable components (Passive devices for LAN)- 12/24 port MM/SM LC LIU Fibre Panel, LC Pigtail SM/MM, LC-LC Multimode/Single mode Patchcord, 6/12/24 core SM OS2 cable, 6/12/24 core OM4 cable etc.	Molex / Systimax / Panduit / D-Link / AMP / R&M
8.	Server Hardware	HP/Dell/Hitachi/IBM
9.	UPS	APC / Emerson/ Merlinzerin / Eaton Powerware