

PACKAGE- 5A

(TECHNICAL SPECIFICATION READ WITH THE CORRECTION SLIP)

**TENDER FOR DATA, NEWTORKING, CCTV, FAS AND ACS WORKS
FOR PERMANENT CAMPUS (PHASE I)
OF**

NALANDA UNIVERSITY, AT RAJGIR, BIHAR.



**TECHNICAL SPECIFICATIONS
(ELV WORKS)**

General: All the material shall must confirm the good working condition as per the local weather/temperature and environmental condition. The product quality must confirm the seismic zone-IV. Before supply of the material lost type test certificate issued by the NABL/NABL accredited laboratory not earlier than 3 years must be submitted for Pre-Despatch Inspection(s).

TECHNICAL SPECIFICATION

1. DATA & TELECOM – PASSIVE CABLING INFRASTRUCTURE – CAT6A CABLE & COMPONENTS, FIBER OPTICS CABLE & COMPONENTS

SCOPE OF WORK

- Complete installation shall be done in accordance with installation practices for a well structured cabling system, using components from a single OEM to ensure consistent and assured performance. The structured cabling distribution network shall serve as a vehicle for transport of data, video and voice telephony signals over a common network throughout the network.
- Devices and services that shall run on the passive network shall include, but not limited to, the following:
 - a.) Wired LAN access
 - b.) Wireless LAN access
 - c.) Voice communications servers and IP/SIP end-points
 - d.) IP-based CCTV/Surveillance Cameras
 - e.) Access Control Controllers
 - f.) DDC controllers for IBMS
 - g.) PLCs, FRTUs and HMI/MMI etc. for SCADA
 - h.) Various devices and controllers for AV system
 - i.) Video-conferencing equipment
- Cabling installation for data and voice communications shall originate at networking racks and terminate at IOs terminated at wall.
- Installation, termination and identification of wiring between station outlets and networking distribution rack(s) and networking distribution rack(s) and main rack (s), shall be considered part of the system integrator's work.
- All cables and terminations shall be tested @500 MHz identified, labelled and documented at all locations.

- The system integrator carrying out the SITC shall make the system entirely operational for its intended use, by addition of components specific to its make/model even if not specifically mentioned in the BoQ without any additional cost.
- System integrator shall provide Ethernet cabling connectivity for all other services, utilities and systems (such as, but not limited to – HVAC, Electrical, Plumbing, Lift Panels and any other such) besides those already forming part of ELV (CCTV, FAS, ACS, Data and Telecom) upto the device location as indicated by the respective utility contractor, e.g., DDCs, PLCs, FRTUs and other such. The respective utility contractor shall indicate the location of their devices and rack where the cabling is to be terminated.

Supported Applications, but not limited to:

- Ethernet Applications – wired Ethernet and wireless as per IEEE 802.11a/b/g/n/ac
- IEEE 802.3af Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)
- Telecom – BRI, PRI and Digital Subscriber Loop (DSL) Applications
- Voice, Video and ISDN Applications

References & Standards, but not limited to:

- TIA / EIA
- International Electro technical Commission (IEC)
- European Committee for Electro technical Standardization (CENELEC)
- American National Standards Institute (ANSI)
- Institution of Electrical and Electronics Engineers (IEEE)
- Wherever there is reference to multiple standards and/codes, the ones most recent and most stringent shall apply.

It shall be the responsibility of the system integrator and OEM manufacturer to ensure that:

- The Passive Components of structured cabling distribution network will be free from manufacturing defects in material and workmanship under normal and proper use.
- All Passive Components in the structured cabling distribution network shall meet or exceed the relevant component specification of the EIA/TIA 568-B and EIA/TIA 568-C.2 series and ISO/IEC 11801: 2002 standards; or later version as applicable at the time of installation.
- The structured cabling distribution network compliant channels will meet or exceed the Guaranteed Channel Performance as per relevant standards in the structured cabling distribution network Performance Specifications in effect at the time of installation.
- The site will be duly certified by OEM for a period of 25 years from the date of issuance of the registration certificate or installation, whichever is earlier, for which they shall submit detailed performance test reports for every IO installed.

- The specifications for items in this section, applies to the following:
 - a.) F/UTP CAT6Acable and associated components such as Patch Panels, IOs/RJ45 Jacks, Patch Cords
 - b.) UTP CAT6 cable and associated components such as Patch Panels, IOs/RJ45 Jacks, Patch Cords
 - c.) Single-Mode fiber optic cable and associated components such as distribution shelves, LIUs, pigtails and patch cords
 - d.) Networking Racks – for termination of networking cables

Installation:

- The final branch connections with single pair cables in conduits and the maximum number of cables in each conduit shall be as follows :

Conduit Diameter	Inch/mm.	Max. No. of cables
1"	25	2 Nos. Of F/UTP CAT6Acables
1½"	40	4 Nos. Of F/UTP CAT6Acables

1.1 F/UTP CAT6ACABLING SYSTEM

No.	Description	Specification
1	Following common specifications shall apply to all F/UTP CAT6A standards based structured cabling components, i.e., Cable, Patch Panel, IOS& Patch Cords. All components of the structured cabling system shall be from the same OEM manufacturer.	
i	Standards Compliance	F/UTP cabling system, conforming to ANSI/TIA/EIA 568-C.2 CAT6A Cabling system, ISO/IEC 11801 2 nd edition, EN-50173-1. The cabling system components must be UL listed or equivalent
ii	Warranty	Performance characteristics shall be provided alongwith the bids and actual tests conducted at site after installation and commissioning for the following parameters: Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4-connector channel. 25-years' systems performance guaranty shall be provided and site shall be certified for guaranteed performance by the OEM/manufacturer along with actual test results conducted at site. The cable shall be tested for minimum guaranteed performance as per standards at 500MHz operation minimum.
iii	OEM Requirement	All passive cabling must be from same OEM (UTP, F/UTP and Fiber)
1.1	F/UTP CAT6A	
i	Standards Compliance	As per 1.i) above
ii	Conductors	23 AWG solid bare copper
iii	Construction and mechanical details	Polyethylene insulation, LSZH jacket.
iv	Operating temperature	-20 Deg. C to +60 Deg. C
v	Delay Skew	Not exceeding 45 ns / 100m
vi	Performance Characteristics	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4-connector channel, to be submitted with bid
1.2	F/UTP CAT6AI/O Jack	
i	Standards Compliance	As per 1.i) above, UL Listed
ii	Performance Characteristics	ETL Verified 4-Connector Channel to ISO/IEC 11801 AMD 1 Class EA, along with channel illustration, and parts numbers to be submitted along with the bid
1.3	F/UTP CAT6APATCH PANEL	
i	Standards Compliance	As per 1.i) above
ii	Ports	24 Ports loaded with shuttered or keystone Jacks
iii	Port arrangement	Individually replaceable jacks or keystone
iv	Height	1 U (1.75 inches)
v	Panel	Fully powder coated
vi	Approvals	UL listed
vii	Termination Pattern	TIA / EIA 568 A and B;
viii	Performance Characteristics	ETL Verified 4-Connector Channel to ISO/IEC 11801 AMD 1 Class EA, along with channel illustration, and parts numbers to be submitted along with the bid
1.4	F/UTP CAT6APATCH CORDS	
i	Standards Compliance	As per 1.i) above
ii	Conductor	24-26 AWG, multi-stranded copper, UL Listed

Iii	Length	Pre-terminated (Factory Crimped) 1 Meter, 2 Meter, 3 Meter options in different colours
1.5	FACEPLATES	
i	Type	1-port, 2 -port or 4-port, White Face plate
ii	Material	ABS / UL 94 V-0
iii	No. of ports	One/ Two / Four

F/UTP CAT6A CABLE LAYING PROCEDURE:

1. The containment system for F/UTP CAT6A cabling shall consist of PVC conduits and multi-compartment raceways. PVC conduits shall be dedicated for all IT/ELV related cabling. Wherever multi-compartment raceways are to be used, the F/UTP cabling for IT/ELV shall be laid in one of the dedicated compartments.
2. An axial spacing of 50 mm (minimum) shall be maintained between power and network cable.
3. If crossing each other, they should be at Right angles. These cables have to be properly tagged & labelled
4. TIA/EIA-569/609 standards have to be followed, while cable laying, considering the conduit fill in ratio, No. of bends, bending radius.
5. Exposed F/UTP cables in horizontal runs are not acceptable.
6. F/UTP cables bunched together with electrical distribution cables or other ELV cables such as fire detection, public address and IBMS signal/communication cables are not acceptable.
7. Proper color coding for I/O identification, has to be followed for field termination. The patch panels & patch cords are supposed to be color coded/Tagged/ identified with stickers (e.g. Blue for data, Yellow for Voice, Violet for IP Surveillance, & Green for Wi-Fi (Stickers on patch panels).
8. Proper earthing/grounding arrangement shall be provided by the ELV System Integrator.
9. Sharp bends such as at 90 degrees are to be avoided – the integrator shall follow OEM guidelines for maintaining bending radii.
10. Cable shall be neatly bundled and dressed to their respective panels or blocks. Each panel or block shall be fed by an individual bundle separated and dressed back to the point of cable entrance into the rack.
11. Each cable shall be clearly labelled on the cable jacket behind the patch panel at a location that can be viewed clearly without removing the bundle support ties. Cables shall be properly marked and distinctively coloured for ease of identification.

1.2 FIBER OPTIC CABLE AND COMPONENTS**SPECIFICATIONS OF SINGLE MODE FIBER OPTIC CABLING SYSTEM:**

ELV SYSTEMS WORKS MATERIAL SPECIFICATIONS FOR NALANDA UNIVERSITY, RAJGIR

i	Type	Single mode OS2 fiber cabling system and all its components; must be from a single OEM (Cables + Components)
ii	Networks Speeds Supported	1Gbps, 10Gbps and 40Gbps
iii	Standard Compliance	ITU-T G.652A, B, C & D, IEC - 60793-2-50, TIA/EIA 568-C.3
iv	Performance Testing	Fiber-channel compliance to ANSI/TIA568 -C.0 for OS2
v	Warranty	25-year systems warranty from OEM including OTDR test reports; Warranty to cover bandwidth of the specified and installed cabling system

SPECIFICATIONS FOR SINGLE MODE OPTICAL FIBER CABLE:

i	Cable Type	6 / 12 / 24 / 48 core, Single Mode, Armored, Loose-unitube for 6 and 12 core , Gel filled&Multi tube construction cable for 24 and 48 core ; typical 6 cores per tube for 24 and 48 core cable
ii	Fiber Type	Single Mode, 9 / 125
iii	Fiber core must be	As per Telecordia GR20, ITU-T G652D, IEC-60793-2-50, TIA/EIA 492-CAAB
iv	No of cores	6 / 12 / 24 / 48 core -ISO 11801 -OS2
v	Aarmor	Corrugated steel tape armor
vi	Cable Construction Type	Loose tube corrugated steel tape armored cable, provided with FRP or equivalent non-metallic central strength member
vii	Outer Jacket Construction	High density polyethylene, anti - termite, anti - rodent suitable for direct burial application. Jacket must be UV stabilized
viii	Losses @ 1310nm frequency	< = 0.4 dB/Km
ix	Losses @1550nm frequency	< = 0.3 dB/Km
x	Operating Temperature	-20 deg C to + 60 deg C
xi	Cable / Component	All fiber cables and components must be from a single OEM (Including F/UTP CAT6ACabling System)
xii	Testing Parameters	Must pass the following : -IEC794-1-E1, IEC794-1-E2, IEC794-1-E3, IEC794-1-E4, EIA-455-104, IEC794-1-E7, IEC794-1-E10, IEC794-1-E11, IEC794-1-F5 or equivalent tests
xiii	Multi-channel capability	The fiber cable must have been designed to provide optimum performance from 1265nm to 1625nm making it suitable for 16 – channel Course Wavelength Division Multiplexing (CWDM) applications

SPECIFICATIONS FOR CONNECTORS:

i	Connector Type	SC or LC-Style, Duplex
ii	Operating temperature	-20 deg C to + 50 deg C
iii	Durability	(500 Matting's): < 0.2 dB Max
iv	Ferrules	Pre-radius Ceramic Zirconia Ferrule. Bayonet Coupling: 2.5 mm Zirconia Ferrule
v	Attenuation	Not more than 0.75 dB per mated pair
vi	Parameters / standard	Meets or exceeds ITU specifications

SPECIFICATIONS FOR PIGTAILS (SINGLEMODE):

i	Type	LC style, SM OS2, Simplex, 1 meter, compliant to ITU-G652.D
ii	Operating temperature	-20 deg C to + 50 deg C
iii	Durability	(500 Matting's): < 0.2 dB Max

ELV SYSTEMS WORKS MATERIAL SPECIFICATIONS FOR NALANDA UNIVERSITY, RAJGIR

iv	Ferrules	Pre-radius ceramic zirconia ferrule. Bayonet coupling: 2.5 mm zirconia ferrule
v	Attenuation	Not more than 0.75 dB per mated pair
vi	Parameters / standard	Meets or exceeds ITU specificationsUL Listed or equivalent

SPECIFICATIONS FOR FIBER OPTIC CABLE PATCHCORDS:

i	Cable type	LC-LC style, SM OS2, available as either 1.6mm or 3mm duplex patch cord. Compliance to ITU-G652.D
ii	Fiber type	Single mode 9/125 micron primary coated buffers
iii	No of cores	2 cable construction type PVC outer jacket
iv	Outside Diameter	1.6mm x 3.0mm (Simplex) or 1.6mm x 3.3mm (Duplex)
v	Operating Temperature	-20 deg C to + 60 deg C

SPECIFICATIONS FOR 19" RACK MOUNTED FIBER OPTIC PATCH PANELS

i	Fiber optic patch panel	19-inch, rack mounted fiber optic patch panel
ii	Height	1U
iii	Number of fiber cores	6/12/24/48 core configurations
iv	Number of OSP (outdoor) cables for termination	Minimum 2
v	Grounding	2 Nos. of earthing lugs
vi	Cable Management rings	Front and rear cable management rings
vii	Adapter plates	6/12/24/48/96 Port adapter plates with each plate loaded with single-mode couplers, as applicable
viii	Construction	Complete Aluminium alloy or CRCA housing, fully powder coated, minimum 1.6mm thick.
ix	Splice tray	Shall be included in LIU

SPECIFICATIONS FOR ADAPTOR PLATES & ADAPTORS (SINGLEMODE):

i	Fiber Optic adapter plate	6-port, SC or LC style
ii	Attenuation	Max of 0.75 dB per mated pair
iii	Adapters	Available in Simplex and Duplex types
iv	Durability	< 0.2 dB max (1000 Matings)
v	Standard	Compliant as per EIA/TIA 568-B and ISO/IES 11080

SPECIFICATIONS FOR EXTERNAL FIBER OPTIC ENCLOSURE:

i	No of fiber core terminations	6/12/24/48 ports
ii	Features	Easy and fast-to-fix for fiber cable termination, IP-68 Rated
iii		Easy to re-enter, it should not require re-entry kits
v		Fiber optic splice tray must be designed in snap in lock & easily fixable.
Vi		Must meet fire codes and industry standards
vii		Should prevent cable sheath movement with temperature changes

FO CABLE LAYING GUIDELINES:

1. Outdoor FO cables shall be buried at a depth of 1200 mm by digging the soil (soft soil as well as hard soil); digging of soil shall be within the scope of ELV contractor; it shall be responsibility of ELV contractor to remake the soil after digging.

2. Where FO cable needs to travel below a road section, the FO cable shall be pulled or laid in pre-laid/existing RCC Hume pipes.
3. While laying FO cables, excessive sharp bends shall be avoided – as a guideline a bending radius of not less than 15 x cable diameter shall be maintained, however, integrator shall follow the OEM's cable laying guideline for the same wherever they are available.
4. Spare cable loop having length of approx. 20 meter shall be left spare inside the manhole chamber for any future jointing, maintenance and extension of branches.
5. The concrete FO route markers shall be specified after every 200m and wherever bends or turns are there in FO route.
6. Each Indoor & Outdoor OS2 Single mode "loose tube" of fiber cable should be properly labeled & marked at all Man holes/ Traps/ Shafts/ LIU end.

1.3 19"WALL MOUNTED NETWORKING ENCLOSURES (6U TO 15U USABLE HEIGHTS)

- Construction shall be single section welded robust with ventilation holes on the sides and top & bottom covers with provision to mount 2 fans
- Top/ Bottom covers and side panels shall be of sheet steel, powder coated
- Vertical 19" metric panel mounts and door trims shall be of sheet steel and powder coated
- The top and bottom covers shall be provided with four cut outs on top and bottom cover for cable entry and round cuts shall be edge protected with rubber grommets
- Two pairs of 19" equipment mounting angles with mounting holes conforming to IEC 297-3
- Toughened glass front lockable door
- Wall mounted 19" Networking rack shall be available in various heights
- Cooling shall be achieved with the help of two fans, 90 CFM capacity each, mounted on top
- Power shall be provided in form 19" rack mountable power strip which shall consist of minimum four 5/15A power sockets. Power strip shall be provided with 20A MCB
- Cantilever shelf – at least one front mounting 1U cantilever shelf shall be provided with depth of 250 mm or more
- 1U vertical cable managers on a/r (as required basis) for dressing of cables for 24 ports patch panel, 24 ports switch
- Hardware Pack / Rack mounting accessories and hardware – as required
- Horizontal managers on A/R basis for ensuring neat and aesthetically clean installation

- Cabinet material – cabinet shall be made of 16 Gauge (1.5mm) thick cold rolled steel sheets or thicker
- Finish – cabinet shall be black or grey epoxy powder-coated of durable quality
- Load carrying capacity – min. 25 kg load of equipment should be mountable
- Product must be UL listed and certified for use in Information Technology or Communication Equipment
- EIA standard pattern design with 12-24 tapped holes (EIA-310-E compliant)
- Dimensions – 6U to 15U usable height, 600mm (W), 450mm(D)

1.4 19" FLOOR STANDING NETWORKING ENCLOSURES (22U TO 42U USABLE HEIGHTS)

- Frame of sturdy frame section construction, consisting of 9 x folded rolled hollow frame section punched in 25mm DIN pitch pattern. All profile edges are radiused. The corners are stiffened with welded zinc die-cast corner connectors, Front and rear perforated door. Top cover with cable entry and Bottom open. 42 U 19" L type angle Front & Rear on 6 x punched section. Cabinet color should be Black and light grey
- The Thickness of the CRCA sheets used for Doors is 1.5mm and for Side Panels is 1.5mm
- Fully adjustable 19" equipment mounting angles
- The cabinet design confirming to DIN 41494 or EIA 310D standards
- Top and Bottom Covers and Side panels shall be of sheet steel and Primary Dip Coat = 20-30 Microns Power Coat = 80-120 Microns
- Vertical 19" metric panel mounts and door trims shall be of sheet steel and powder coated
- The Top cover with min. 4 cut out of diameter 100mm or more for cable entry. Bottom cover with 4 cut out of diameter 100mm or more for cable entry. All cut outs blanked with plastic caps
- Perforation - for full / split perforated doors the style should be "Honeycomb" type of perforation for maximum air circulation and stiffness. Doors should have min. 75% perforation for better air circulation
- Cabinet shall be capable of dismantling and reassemble at the site
- Locks options – options shall be available such as slam lock - common key or unique key, Swing handle lock, Digital Keypad operated locks, Biometric locks
- Side panels – must contain slam latches for locking purpose and option of providing slam locks, or screw fitted for removal, if required
- Two pairs of 19" Equipment mounting angles with mounting holes conforming to IEC 2973
- Front glass door made of toughened glass, tinted with easily detachable hinges

- Two pairs of slotted vertical cable channel shall be provided at front and back for managing cables
- Lockable industrial grade castors with foot brakes
- Rack shall be supplied with 4 x 90 CFM fans at top
- Rack shall be supplied with equipment mounting hardware in pack of 20s such as mounting nuts and screws either 12-24 or M6 type as applicable
- Minimum 2 nos. of 8 x 5/15 Amps power supply sockets, 2 nos. of vertical cable managers and 2 no. of 19" 1U size horizontal cable managers
- Finish – cabinet shall be black or grey epoxy powder-coated of durable quality. The Powder coating of the racks is as per Nano coated, electro-dip coat primed to 20 microns, and power coated with texture polyester with 80 to 120 microns for long lasting paint against corrosion
- Product must be UL listed and certified for use in Information Technology or Communication Equipment
- EIA standard pattern design with 12-24 tapped holes (EIA-310-E compliant) or EIA standard pattern design with 3/8" (9.5mm) square punches for Cage Nuts for mounting

2. ACTIVE COMPONENTS - NETWORKING SWITCH SPECIFICATIONS

DESCRIPTION & DESIGN

- Campus networking infrastructure is a high performance design that factors important parameters such as aggressive use of IT and e-Learning in education, scalability and reliability.
- Key considerations for network are – gigabit connectivity to each user from the nearest distribution rack to various users/departments/devices in a topology consisting of core switches at central server room followed by the distribution and edge/access switches.
- The network shall have a mix of components for supporting PoE+ as well as non-PoE devices.
- A robust fiber optics based backbone is being provided. It shall be based on ring topology using single mode fiber optics cable. The vendor shall ensure that the networking switches shall be populated with the necessary transceivers for achieving this design objective.
- Several applications are proposed to run on this network – IP-based voice communications supporting voice-data-video, network based cameras and storage, integrated audio-video, video conferencing, interactive learning, integrated building management systems and important services integration such as fire detection.
- The integrators shall propose and supply enterprise class networking switches only.

2.1. TYPE-1 EDGE SWITCH (ACCESS SWITCH)

Layer 2, 8 x 10/100/1000 Base-Tx Ports, PoE+, plus minimum 2 dedicated SFP Ports

Switch Architecture

- The switch should have 8 X 10/100/1000 Base-Tx ports; all ports shall be 802.3at-compliant PoE+ capable, with the switch capable of providing minimum 120 Watts of PoE power budget.
- The switch should also support PoE as per 802.3af on all ports.
- Switch should have 8 Nos. 10 Base-T/100Base-Tx/1000Base-Tx auto-sensing ports complying to IEEE 802.3, IEEE 802.3at, IEEE 802.3u and 802.3ab standard, supporting half duplex mode, full duplex mode and auto-negotiation on each port.
- Switch should have minimum 2 dedicated SFP ports.
- The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire-speed / line-rate. Switching fabric capacity of the switch should be capable to run all the ports at line-rate.
- Switch should support both IPv4 and IPv6 – Switch should support features like Neighbour Discovery, Syslog, Telnet, SSH, Web GUI, SNMP, NTP, DNS, RADIUS over IPv6
- Switch should have non-blocking switching bandwidth of minimum 24Gbps.
- Switch should have forwarding rate of minimum 14Mpps.
- Switch should be IPv6-Ready from Day 1

Layer 2 Features

- IEEE 802.1Q VLAN tagging
- 802. 1Q VLAN on all ports with support for minimum 255 VLANs.
- Support for minimum 8k MAC addresses.
- Spanning Tree Protocol as per IEEE 802.1d.
- Multiple Spanning-Tree Protocol as per IEEE 802.1s.
- Rapid Spanning-Tree Protocol as per IEEE 802.1w.
- Self-learning of unicast & multicast MAC addresses per switch port.
- Jumbo frames up to 9000 bytes.
- Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.

Security Features

- Switch should support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports.
- Switch should support Port based Filters / ACLs.
- Switch should support RADIUS and TACACS+ for access restriction and authentication.
- Secure Shell (SSH) Protocol, HTTP and DoS protection.
- ARP spoofing, DHCP snooping etc.
- Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard.

Management Features

- The switch should support CLI as well as web-based Management.
- Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
- Switch should support all the standard MIBs (MIB-I & II).
- Switch should support TELNET and SSH Version-2 for Command Line Management.
- Switch should support 4 groups of embedded RMON (history, statistics, alarm and events).

- Switch should support System & Event logging functions as well as forwarding of these logs to multiple syslog servers.
- Switch should support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS should not require rebooting of the switch.
- Switch should have comprehensive debugging features required for software & hardware fault diagnosis.
- Switch should support multiple privilege levels to provide different levels of access.
- Switch should support SNTP (Network Time Protocol).
- Switch should support FTP/TFTP for software upgrade.
- Switch support multiple configuration file & backup configuration file.

2.2. TYPE-2 EDGE SWITCH (ACCESS SWITCH)

Layer 2, 24 x 10/100/1000Base-Tx Ports, PoE+, minimum 4 dedicated SFP Ports. All 28 ports should be active simultaneously

Switch Architecture

- The switch should have 24 X 10/100/1000 Base-Tx ports; all ports shall be 802.3at-compliant PoE+ capable, with the switch capable of providing minimum 350 Watts of PoE power budget.
- The switch should also support PoE as per 802.3af on all ports.
- Switch should have 24 Nos. 10 Base-T/100Base-Tx/1000Base-Tx auto-sensing ports complying to IEEE 802.3, IEEE 802.3at, IEEE 802.3u and 802.3ab standard, supporting half duplex mode, full duplex mode and auto-negotiation on each port.
- **Switch should have minimum 4 dedicated**
- The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire-speed / line-rate. Switching fabric capacity of the switch should be capable to run all the ports at line-rate.
- Switch should support auto switch replacement in an existing stack with the new switch without any configuration for joining the stack
- Switch should support link aggregation across multiple switches in a stack.
- Switch should support both IPv4 and IPv6 – Switch should support features like Neighbour Discovery, Syslog, Telnet, SSH, Web GUI, SNMP, NTP, DNS, RADIUS over IPv6
- Switch should have non-blocking switching throughput of minimum 52Gbps.
- Switch should have forwarding rate of minimum 35Mpps.
- Switch should be IPv6-Ready from Day 1
- Switch should have the capabilities to stack upto 8 switches with dedicated stacking port/ virtual chassis from day 1 and with minimum stacking bandwidth of 80Gbps

Layer 2 Features

- IEEE 802.1Q VLAN tagging
- 802. 1Q VLAN on all ports with support for minimum 255 VLANs.
- Support for minimum 16k MAC addresses.
- Spanning Tree Protocol as per IEEE 802.1d.
- Multiple Spanning-Tree Protocol as per IEEE 802.1s.
- Rapid Spanning-Tree Protocol as per IEEE 802.1w.
- Self-learning of unicast & multicast MAC addresses per switch port.
- Jumbo frames up to 9000 bytes.
- Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.

Quality of Service (QOS) Features

- Switch should support classification and scheduling as per IEEE 802.1P on all ports.
- Switch should support four queues per port.
- Switch should support QoS configuration on per switch port basis.
- Switch should provide traffic shaping and rate limiting features (for egress as well as ingress traffic).

Security Features

- Switch should support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports.
- Switch should support Port based Filters / ACLs.
- Switch should support RADIUS and TACACS+ for access restriction and authentication.
- Secure Shell (SSH) Protocol, HTTP and DoS protection.
- ARP spoofing, DHCP snooping etc.
- Switch should support static ARP, Proxy ARP, UDP forwarding and IP sourceguard.

Management Features

- The switch should support CLI as well as web-based Management.
- Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
- Switch should support all the standard MIBs (MIB-I & II).
- Switch should support TELNET and SSH Version-2 for Command Line Management.
- Switch should support 4 groups of embedded RMON (history, statistics, alarm and events).
- Switch should support System & Event logging functions as well as forwarding of these logs to multiple syslog servers.
- Switch should support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS should not require rebooting of the switch.
- Switch should have comprehensive debugging features required for software & hardware fault diagnosis.
- Switch should support multiple privilege levels to provide different levels of access.
- Switch should support NTP (Network Time Protocol).
- Switch should support FTP/TFTP for software upgrade.
- Switch support multiple configuration file & backup configuration file.

2.3. TYPE-3 BLOCK/CLUSTER DISTRIBUTION SWITCH

Layer 3, 24 x 1G SFP Ports, 4 x 10G SFP+ Ports, Redundant Power Supply, Redundant Fan, Full Advanced L3 Features

Switch Architecture

- The switch should have at least 24Nos. 1G Base- SFP ports
- The switch should have at least 4 Nos. 10G - SFP+ ports
- The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire-speed / line-rate. Switching fabric capacity of the switch should be capable to run all the ports at line-rate
- The switch should support both IPv4 and IPv6 – Switch should support features like Neighbour Discovery, Syslog, Telnet, SSH, Web GUI, SNMP, NTP, DNS, RADIUS overIPv6
- The switch should have non-blocking switching bandwidth of minimum 128Gbps
- The switch should have forwarding rate of minimum 80Mpps
- The switch shall be supplied with at least one redundant power supply
- The switch shall be supplied with at least one redundant fan
- The switch should be IPv6 Ready from day 1

Supported Layer 2 Features

- IEEE 802.1Q VLAN tagging
- 802.1Q VLAN on all ports with support for minimum 1000 VLANs
- Support for minimum 32K MAC addresses
- Spanning Tree Protocol as per IEEE 802.1d
- Multiple Spanning-Tree Protocol as per IEEE 802.1s
- Rapid Spanning-Tree Protocol as per IEEE 802.1w
- Jumbo frames up to 9000 bytes
- Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
- QoS Prioritization as per IEEE 802.1p
- User Authentication as per IEEE 802.1x

Supported Layer 3 Features

- The Layer 3 switch should support full Layer 3 features like PIM-DM/, PIM-SM, RIPv1/v2, OSPF, PBR, ECMP, BGP and VRRP; it shall be supplied with all requisite licences for implementing Layer 3 capabilities
- The Layer 3 Switch should support for full IPv6 features like RIPv6, MLD v1/v2, OSPFv3, VRRPv3 and IPv6 management
- The Distribution switch should support virtualization routing and forwarding
- Inter-VLAN IP routing for full layer 3 routing between two or more VLANs
- IP unicast routing protocols (static, RIPv1/v2 & OSPF)
- Virtual Router Redundancy Protocol (VRRP) as per RFC 3768 or equivalent
- Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping or Proxy
- Switch should support up to 512 multicast groups/entries
- Inter-VLAN IP routing for full layer 3 routing between two or more VLANs

Security Features:

- Switch should support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports
- Switch should support Port based Filters / ACLs
- Switch should support RADIUS and TACACS+ for access restriction and authentication
- Secure Shell (SSH) Protocol, HTTP and DoS protection
- IP Route Filtering, ARP spoofing, DHCP snooping
- Switch should support static ARP, Proxy ARP, UDP forwarding and IP source-guard

Management Features

- The switch should support CLI based or Web-based Management, via a console port
- Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3
- Switch should support all the standard MIBs (MIB-I& II)
- Switch should support TELNET and SSH Version-2 for Command Line Management
- Switch should support 4 groups of embedded RMON (history, statistics, alarm and events)
- Switch should support System & Event logging functions as well as forwarding of these logs to multiple syslog servers
- Switch should support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS should not require rebooting of the switch
- Switch should have comprehensive debugging features required for software & hardware fault diagnosis
- Switch should support multiple privilege levels to provide different levels of access
- Switch should support NTP (Network Time Protocol)
- Switch should support FTP/TFTP for software upgrade
- Switch support multiple configuration file & backup configuration file

2.4. TYPE-4CORE SWITCH

Layer 3, 24 x 10G SFP+ Ports, 2 x 40G QSFP+ Ports, Redundant Power Supply, Redundant Fan, Full Advanced L3 Features

Switch Architecture

- The switch should have at least 24Nos. 10G Base- SFP+ ports
- The switch should have at least 2 Nos. 40G - QSFP+ ports
- The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire-speed / line-rate. Switching fabric capacity of the switch should be capable to run all the ports at line-rate
- The switch should support both IPv4 and IPv6 – Switch should support features like Neighbor Discovery, Syslog, Telnet, SSH, Web GUI, SNMP, NTP, DNS, RADIUS overIPv6
- The switch should have non-blocking switching bandwidth of minimum 600Gbps
- The switch should have forwarding rate of minimum 440Mpps
- The switch shall be supplied with at least one redundant power supply
- The switch shall be supplied with at least one redundant fan
- The switch should be IPv6 Ready from day 1
- Switch should have the capabilities to stack upto 8 switches with dedicated stacking port/ virtual chassis from day 1 and with minimum stacking bandwidth of 240Gbps

Supported Layer 2 Features

- IEEE 802.1Q VLAN tagging
- 802. 1Q VLAN on all ports with support for minimum 1000 VLANs
- Support for minimum 32K MAC addresses
- Spanning Tree Protocol as per IEEE 802.1d
- Multiple Spanning-Tree Protocol as per IEEE 802.1s
- Rapid Spanning-Tree Protocol as per IEEE 802.1w
- Jumbo frames up to 9000 bytes
- Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
- QoS Prioritization as per IEEE 802.1p
- User Authentication as per IEEE 802.1x

Supported Layer 3 Features

- The Layer 3 switch should support full Layer 3 features like PIM-DM/, PIM-SM, RIPv1/v2, OSPF, PBR, ECMP, BGP and VRRP; it shall be supplied with all requisite licences for implementing Layer 3 capabilities
- The Layer 3 Switch should support for full IPv6 features like RIPng, MLD v1/v2, OSPFv3, VRRPv3 and IPv6 management
- The Distribution switch should support virtualization routing and forwarding
- Inter-VLAN IP routing for full layer 3 routing between two or more VLANs
- IP unicast routing protocols (static, RIPv1/v2 & OSPF)
- Virtual Router Redundancy Protocol (VRRP) as per RFC 3768 or equivalent
- Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping or Proxy
- Switch should support up to 512 multicast groups/entries
- Inter-VLAN IP routing for full layer 3 routing between two or more VLANs

Security Features:

- Switch should support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports
- Switch should support Port based Filters / ACLs
- Switch should support RADIUS and TACACS+ for access restriction and authentication
- Secure Shell (SSH) Protocol, HTTP and DoS protection
- IP Route Filtering, ARP spoofing, DHCP snooping
- Switch should support static ARP, Proxy ARP, UDP forwarding and IP source-guard

Management Features

- The switch should support CLI based or Web-based Management, via a console port
- Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3
- Switch should support all the standard MIBs (MIB-I& II)
- Switch should support TELNET and SSH Version-2 for Command Line Management
- Switch should support 4 groups of embedded RMON (history, statistics, alarm and events)
- Switch should support System & Event logging functions as well as forwarding of these logs to multiple syslog servers
- Switch should support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3functions, VLAN, STP, Security, QoS should not require rebooting of the switch
- Switch should have comprehensive debugging features required for software &hardware fault diagnosis
- Switch should support multiple privilege levels to provide different levels of access
- Switch should support SNTP (Network Time Protocol)
- Switch should support FTP/TFTP for software upgrade
- Switch support multiple configuration file & backup configuration file

2.5. WIRELESS LAN INFRASTRUCTURE (CONTROLLER AND ACCESS POINT)

2.5.1. ARCHITECTURE

- Wireless deployment should be on a centralised controller-based architecture with the controller in High Availability mode providing seamless scalability
- The architecture should be scalable to support 1000APs in the campus
- Redundancy should be built in the architecture, i.e., 1+1 controller configuration. Redundancy should be built in the architecture where there is no single point of failure
- Solution should support application visibility and control
- Should support Band Steering/Band Select to force clients with dual band support to register to only 5Ghz, thus freeing up capacity in 2.4Ghz
- Supports complete local AAA authentication and including 802.1x as primary or backup to a centralized AAA server
- It should have Internal Captive Portal including support for external CP
- The WLAN APs must support either internal RADIUS server or external RADIUS servers for user authentication
- Solution should support Campus or Public Cloud mode of management for Management and Control
- Solution should also support Hotspot 2.0 (IEEE 802.11u)
- Should support IEEE 802.1x with multiple EAP types (TLS or EAP/MSCHAP or TTLS or equivalent)
- Wireless system should support IPv6 from Day 1
- Radio Resource Management capabilities for radio self-test and healing shall be supported by the solution
- Wireless solution shall support IEEE 802.1q – VLAN Tagging
- Wireless solution shall support IEEE 802.1p – Layer 2 Traffic Prioritization
- Wireless solution shall support IPv6 Control for an increased wireless device density through control of unnecessary IPv6 traffic on IPv4-only networks
- Solution must have capabilities to set a maximum per-user bandwidth limit on per-SSID basis

2.5.2. WIRELESS CONTROLLER

- The controller shall have two 10Gb ports
- The controller shall support 1500 access points without hardware change
- Shall support 15,000 users from day one
- Shall support 1+1, N+1, N+N redundancy models
- The primary controller should have the capabilities to cater all the APs independently and in case of any failure the secondary/redundant controller should take entire load

WLAN controller management features

- Shall support spectrum analysis from day one - to detect and mitigate non Wi-Fi interference
- Shall support band navigation/band select functionality to enable redirection of 5Ghz clients to 5Ghz radio
- Shall support VLAN pooling which ensures assignment of VLANs to SSID
- Shall support AP grouping to enable an admin to easily apply AP-based or radio-based configurations to all the APs that are in the same group
- Controller/Solution should have basic profiling capabilities
- Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyse information about applications usage, peak network usage times for all access points from day one in a central and local switching mode

WLAN controller security features

- WLC should detect if someone connects a Rogue Access Point in network and should be able to take appropriate action to contain rogue Access point.
- WLC should detect and protect an Ad-hoc connection when a connected user attempts forming a network with other system without an AP or try enabling bridging between two interfaces.
- WLC should detect and take appropriate containment action if a smartphone user uses tethering to connect other device.
- WLC should detect and protect if a user attempts to spoof MAC address of valid client or AP for unauthorized access/authentication.
- Shall support integrated system of detection for wireless intrusion from day one
- Controller should support Rogue AP detection and classification and should have WIPs signatures

WLAN controller performance features

- Shall support layer 3 roaming and fast roaming
- Shall support airtime fairness
- Shall support client load balancing based on sessions and traffic load
- Shall support bandwidth limiting per SSID

2.5.3. WIRELESS LAN MANAGEMENT

- WMS should support following broad life cycle management features:
 - i. Configuration and policy management
 - ii. Performance monitoring
 - iii. Reporting and analytics
 - iv. Security monitoring
 - v. Troubleshooting
- WMS should support following key features:
 - i. Web-Based Interface
 - ii. Network Discovery
 - iii. Detailed AP Status
 - iv. Station Troubleshooting
 - v. Policy Configuration
 - vi. Wireless Heat Maps
 - vii. Security Monitoring
 - viii. 802.11 Packet Capture
 - ix. Device Identification
 - x. Reporting
- WMS dashboard should provide real time summary of status and activity based on parameters such as:
 - i. AP and Radio Status
 - ii. AP/Radio Throughput
 - iii. Rogue & Threat Overview
 - iv. Most Recent Alarms
 - v. Station Information
- It should be possible to drill down to individual AP station(s) for troubleshooting and proactive station monitoring, alerting on errors, rates, signal levels
- It should be possible to Assign and configure newly discovered Wireless APs with default or pre-selected policies & Configuration templates applied to individual or AP groups
- Solution should support Layer 2 and Layer 3 roaming

- It should be possible to locate function in map showing station location & Use signal from multiple APs for location identification & should also display station/rogue details
- WMS should have ability to display heat maps and clients
- Wireless solution should support techniques for automation of configuration and service provisioning & also simplify adds, moves, and changes of authenticated and authorized network endpoints
- Wireless solution should support complete AAA authentication, including 802.1x, as primary or backup to a centralized AAA server
- WMS Software should be installable on an VM environment or appliance
- WMS should have functionality to generate graphical maps showing wireless coverage heat maps, devices and location
- Solution should support troubleshooting tools, packet capture and reports to resolve connectivity and performance issues
- Solution should allow automated deployment of new software image to one or more APs, or groups of APs for centralized management through controller
- Customizable view listing security events by type, detected by APs, with time detected, MAC address of device and SSID or AP name.
- Web access (https) for configuration, SNMP v1, v2c, v3
- Syslog support for system monitoring

2.5.4. ACCESS POINT

- Dual Radio, with 802.11a/n/ac (5 GHz) and 802.11g/n (2.4 GHz) concurrent operation
- 4X4:3 Multiple Input / Multiple Output (MIMO) Wave 2 access point
- Internal/external antennas for 2.4GHz and 5GHz operations with one 10/100/1000 Base-Tx auto-sensing (RJ45) PoE+ port
- AP must have two radios (2.4GHz or 5GHz)
- Maximum Associated Users: 240 (120 per radio)
- AP must have two ethernet ports for link aggregation
- Power Supply: via an 802.3at POE+ switch port or OEM supplied Power Injector
- Access point should be 802.11ac Wave 2 from day 1
- IEEE 802.3 10-BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, IEEE 802.3ab 1000BASE-T
- AP must include OEM supplied mounting brackets and accessories for various mounting options such as ceiling, wall or rooftop

Security:

- WPA
- IEEE 802.11i WPA2
- RFC 2246 TLS protocol version 1.0
- RFC 3280 Internet X.509 PKI certificate and CRL profile
- RFC 4346 TLS protocol version 1.1/1.0

Encryption:

- TKIP-MIC: RC4 40 bit, 104 bit and 128 bit, SSL & TLS: RC4 128-bit
- PHY data rates up to 1.8Gbps per AP
- Support for band steering, client load balancing, LLDP
- Should support 802.1X authentication
- Should support centralized configuration and management and reporting
- Solution should have Bonjour Support for supporting Apple devices
- Should support Wi-Fi Alliance Protected Access 1.0 (WPA) and 2.0 (WPA2)

2.6. CENTRALISED NETWORK MANAGEMENT AND MONITORING SOFTWARE

Network Discovery

- GUI based system (Web based & Windows Based)

- **Auto - discovery**

- Discovery of network elements should be on per device basis and it should be possible to import L2 and L3 topologies
- System should support the discovery of devices from Layer -2 to Layer -3 devices
- System should have the capability to capture logical connectivity information including virtual private network (VPN)
- All licenses, required if any, for registering and managing all manageable devices as per the BoQ scope shall be provided by the vendor/integrator
- The network management platform shall provide a single integrated solution for comprehensive lifecycle management of the wired/wireless access, campus, and branch networks, and rich visibility into end-user connectivity and application performance assurance issues.
- System should support Automated configuration deployment and automated staging capability

Fault Management

- System should support comprehensive fault management for all the network devices
- Should give event details & be capable of suppressing fault by launching fault summary
- System should be able to monitor & troubleshoot problems at the protocol level
- The system shall be capable of pre-provisioning with base lined configuration & image

Performance Management

- System should give real time utilization and performance matrix
- **System should provide facility to track the performance matrix on subnet or VLAN basis and protocol basis**
- System should support wireless LAN Management
- System should be able to deliver highly accurate, real-time information on network connectivity, availability, performance, usage, and inventory
- System should be able to monitor, track the up/down status, and analyze real-time, in-depth, network performance statistics for routers, switches, wireless access points, and any other SNMP-enabled device
- System should be able to provide a device-by-device drill down and detailed system information on network devices and virtual switches

Security Management

- Should support AAA server and user access management for BYOD functionality for minimum 5000 concurrent users with complete Guest life cycle management and should have minimum 3000 devices license from day 1
- Should support inventory management on per device basis
- Should be able handle Alert/Event management
- Should support workflows for improved setup and troubleshooting
- System should offer centralized change – audit logging, graphical device management

Guest Life Cycle Management

- The Solution should have AAA functionality and Guest Life Cycle Management in redundant mode (Bidder should propose any additional hardware if required)
- Network Management and Monitoring entity should have the capabilities to launch and integrate AAA functionality

Description ADDED as follows at the end of last paragraph:

3. VIDEO SURVEILLANCE SYSTEM

GENERAL

- The Surveillance System components must be TCP/IP based components working on the same backbone network as the Data Network (LAN).
- Surveillance system must be scalable in terms of equipment (no. of cameras), storage capacity and licenses.
- True open platform functionality is an essential aspect of this specification; cameras from different OEMs must be able to integrate seamlessly with the specified 3rd party VMS software platforms without any loss of features and functionality. Similarly, supplied VMS software platforms must also be able to integrate with a variety of cameras from different manufacturers in future.
- For better saving on storage and bandwidth the compression used shall be H.264 high profile for all types of cameras and devices. H.264 high profile shall be a common requirement for all cameras and devices irrespective of whether mentioned in individual sub-sections or not or if mentioned otherwise.
- All cameras shall be vandal resistant as per IK10 rating.
- All cameras shall be ONVIF Profile S compliant
- Cameras shall have a wide dynamic range of between 85 to 95dB (for Fixed Box/CS-Mount and Indoor Dome/Mini-dome models and between 120 to 130dB (for indoor/outdoor PTZ models)for ensuring good image performance in varying light conditions.
- **"All cameras shall be UL listed/certified"**

3.1. FULL HIGH DEFINITION, TRUE DAY/NIGHT, INDOOR NETWORK RAPID PTZCAMERA

GENERAL REQUIREMENTS:

- The camera shall be a Full HD Rapid Dome PTZ camera supporting triple streaming of codecs; simultaneously generating and transmitting JPEG/MJPEG and two independent H.264High Profile video streams different in resolutions and frame rates.
- The camera shall have a 1/3" type CMOS/CCD/MOS sensor of approx. 2.0 Megapixels and have a True day/night capability.
- The camera shall be capable of 360 degree pan rotation and a minimum tilt range of 0° to 180°, designed for ceiling mount operation.
- The camera shall incorporate a built-in 30X optical, auto-focus zoom lens, and shall have 12X digital zoom capability with 360X total zoom capability.
- The camera shall be able to automatically sequence through the preset positions in programmable sequence, i.e., preset tours.
- The camera shall produce a high quality picture with a minimum illumination of 0.4 lux in color mode or 0.02 lux in B/W mode at F1.6 or better. It shall offer IR cut filter that switches on/off to enhance low-light sensitivity during B/W mode.
- The camera shall be equipped with an intelligent automatic backlight compensation capability, mask settings and level adjustment capabilities to compensate for backlight by masking out brighter areas.
- The camera shall have feature to transform shadows and dark areas into natural and crisp images in real time.
- The camera shall support automatic tracing white balance adjustment capability.
- The camera shall have light control mode to select the operating environment, i.e., indoor or outdoor.
- The camera shall have a 2D and 3D noise reduction capability for reducing AGC noise to provide clear images without motion blur.
- The network interface shall be an 8-pin RJ-45 connector, 10Base-T/100Base-TX Ethernet. Both IPv6 and IPv4 shall be supported.
- The camera shall support JPEG/MJPEG and H.264 high profile compression. The minimum resolution for each codec shall be 1920 x 1080
- The camera shall be capable of generating HTML code for the video image, allowing for easy web page integration.
- The camera shall be capable of supporting up to five (05) users simultaneously over the network.
- The camera shall have the capability to stream JPEG/MJPEG and H.264 high profile video in TCP protocol H.264 in UDP (unicast/multicast) protocol.
- The camera shall incorporate a built-in algorithm for intelligent motion detection capability. The camera shall offer this feature with minimum four configurable areas per scene and ten sensitivity levels adjustments.

- The camera shall have 2-way audio features, i.e., the camera shall have built-in audio input and output jacks and be capable of transmitting and receiving full duplex audio stream on the same Ethernet connection as the video. The audio shall be encoded using the G.726 or equivalent ADPCM standard.
- The camera shall support the following network protocols: TCP/IP, UDP/IP, HTTP, HTTPS, RTSP, RTP, RTP/RTCP, FTP, SMTP, DHCP, DNS, DDNS, NTP, SNMP, UPnP
- The camera shall support HTTPS client authentication.
- The camera shall be compliant with the industry standard ONVIF (Open Network Video Interface Forum) specification with Profile S compliance.
- The camera shall have user configurable port settings.
- The camera shall have an email (SMTP) notification capability and shall support scheduled transfer of image data via FTP to an FTP server.
- The camera shall have privacy zone masking for blocking out unwanted or prohibited areas within the video image to protect privacy.
- The camera software should include IP Setup (including group camera management) program, Firmware Upgrade Tool, Privacy Masking Tool. The software shall be supplied with the camera as a standard accessory.
- The minimum electronic shutter setting shall be 1 second, and a maximum of 1/20,000 sec.
- The camera shall have minimum 2 external I/O Terminals for external alarms and/or controls
- The camera shall be capable of limiting bandwidth from 64 kbps to 8 Mbps in H.264 mode while also being able to operate without bandwidth limitation in JPEG format.
- The camera shall be capable of automatically transmitting alarm images transfer via FTP file transfer and/or e-mail. In addition the network camera shall support scheduled transfer of image information via FTP to an FTP server.
- Terminal inputs, video motion detection alarms, and alarm commands shall be able to trigger actions such as memory recording, FTP file transfer, e-mail notification, alarm indications on web browser, alarm terminal output, and alarm command.
- The camera shall have a local storage capability via a memory card slot which can support up to 64GB memory card that can cache images in the event of a network failure. The camera shall also support manual/alarm recording to the optional memory card. The camera shall provide notification of the remaining capacity of the memory card.

CAMERA LENS SPECIFICATIONS:

- The camera shall have an integrated minimum 30X auto-focus zoom lens.
- Focal length shall be 4.3 mm (+/- 10%) to 129 mm (+/- 10%) with field of view coverage of 2.4° (+/- 10%) to 63.5° (+/- 10%).
- The aperture range for the lens shall be F1.6 to F4.7 (+/- 10%).

VIDEO-ELECTRICAL REQUIREMENTS:

- The camera input power shall be PoE+ or optionally AC/DC 24V which shall be included in supply, if necessary.

AUDIO REQUIREMENTS:

- The camera shall support bi-directional audio, using G.726 or equivalent 16KHz sampling standards such as AAC.
- It shall support audio modes such as - OFF or Mic (Line) input or Audio output or Interactive (Half duplex) or Interactive (Full duplex)
- The camera shall have mini-jack connectors accessible via pigtail to support external microphone and active speakers.

MECHANICAL REQUIREMENTS:

- The camera shall have 360° endless pan rotation and 0° to 180° tilt range. The unit shall be designed for ceiling mount operation.
- The camera shall have pan/tilt speeds of 300° per second in presets
- The camera shall have onehundred (100) user defined presets.
- The camera shall be vandal resistant with IK10 rating or IEC 62262 compliance.
- The camera shall have inbuilt dehumidification/defog feature to remove moisture.

3.2. FULL HIGH DEFINITION, TRUE DAY/NIGHT, OUTDOOR NETWORK RAPID PTZ CAMERA**GENERAL REQUIREMENTS:**

- The camera shall be a Full HD Rapid Dome PTZ camera supporting triple streaming code simultaneously generating and transmitting JPEG/MJPEG and two independent H.264 High Profile video streams different in resolutions and frame rates.
- The camera shall have a 1/3" type CMOS/CCD/MOS sensor of approx. 2.0 Megapixels and have a True day/night capability.
- The camera shall be capable of 360 degree pan rotation and a minimum tilt range of 0° to 180°, designed for ceiling mount operation.
- The camera shall incorporate a built-in 30X optical, auto-focus zoom lens, and shall have 12X digital zoom capability.
- The camera shall be able to automatically sequence through the preset positions in programmable sequence, i.e., preset tours.
- The camera shall produce a high quality picture with a minimum illumination of 0.6 lux in color mode or 0.07 lux in B/W mode at F1.6 or better. It shall offer IR cut filter that switches on/off to enhance low-light sensitivity during B/W mode.
- The camera shall be equipped with an intelligent auto backlight compensation capability, mask settings and level adjustment capabilities to compensate for backlight by masking out brighter areas.
- The camera shall have feature to transform shadows and dark areas into natural and crisp images in real time.
- The camera shall support automatic tracing white balance adjustment capability.

ELV SYSTEMS WORKS MATERIAL SPECIFICATIONS FOR NALANDA UNIVERSITY, RAJGIR

- The camera shall have light control mode to select the operating environment, i.e., indoor or outdoor.
- The camera shall have a 2D and 3D noise reduction capability for reducing AGC noise to provide clear images without motion blur.
- The network interface shall be an 8-pin RJ-45 connector, 10Base-T/100Base-TX Ethernet. Both IPv6 and IPv4 shall be supported.
- The camera shall support JPEG and H.264 high profile compression. The minimum resolution for each codec shall be 1920x1080.
- The camera shall be capable of generating HTML code for the video image, allowing for easy web page integration.
- The camera shall be capable of supporting up to five (05) users simultaneously over the network.
- The camera shall have the capability to stream JPEG/MJPEG and H.264 high profile video in TCP protocol H.264 in UDP (unicast/multicast) protocol.
- The camera shall have built-in motion detection capability.
- The camera shall have 2-way audio features, i.e., the camera shall have built-in audio input and output jacks and be capable of transmitting and receiving full duplex audio stream on the same Ethernet connection as the video. The audio shall be encoded using the G.726 or equivalent 16KHz sampling rate standards such as AAC.
- The camera shall support the following network protocols: TCP/IP, UDP/IP, HTTP, HTTPS, RTSP, RTP, RTP/RTCP, FTP, SMTP, DHCP, DNS, DDNS, NTP, SNMP, UPnP.
- The camera shall support HTTPS client authentication.
- The camera shall be compliant with the industry standard ONVIF (Open Network Video Interface Forum) specification with Profile S compliance.
- The camera shall have user configurable port settings.
- The camera shall have an email (SMTP) notification capability and shall support scheduled transfer of image data via FTP to an FTP server.
- The camera shall have privacy zone masking for blocking out unwanted or prohibited areas within the video image to protect privacy.
- The camera software should include IP Setup (including group camera management) program, Firmware Upgrade Tool, Privacy Masking Tool. The software shall be supplied with the camera as a standard accessory.
- The minimum electronic shutter setting shall be 1 second, and a maximum of 1/20,000 sec.
- The camera shall have minimum 2 external I/O Terminals for external alarms and/or controls.
- The camera shall be capable of limiting bandwidth from 64 kbps to 8 Mbps in H.264 mode while also being able to operate without bandwidth limitation in JPEG format.
- The camera shall be capable of automatically transmitting alarm images transfer via FTP file transfer and/or e-mail. In addition the network camera shall support scheduled transfer of image information via FTP to an FTP server.

- Terminal inputs, video motion detection alarms, and alarm commands shall be able to trigger actions such as memory recording, FTP file transfer, e-mail notification, alarm indications on web browser, alarm terminal output, and alarm command.
- The camera shall have a local storage capability via a memory card slot which can support up to 64GB memory card that can cache images in the event of a network failure. The camera shall also support manual/alarm recording to the optional memory card. The camera shall provide notification of the remaining capacity of the memory card.
- The camera shall have built-in motion detection capability.

CAMERA LENS SPECIFICATIONS:

- The camera shall have an integrated minimum 30X auto-focus zoom lens.
- Focal length shall be 4.3 mm (+/- 10%) to 129 mm (+/- 10%) with field of view coverage of 2.4° (+/- 10%) to 63.5° (+/- 10%).
- The aperture range for the lens shall be F1.6 to F4.7 (+/- 10%).

VIDEO-ELECTRICAL REQUIREMENTS:

- The camera input power shall be PoE+ or optionally AC/DC 24V which shall be included in supply, if necessary.
- Power consumption SHOULD be minimum confirming the required features.

AUDIO REQUIREMENTS:

- The camera shall support bi-directional audio, using G.726 or equivalent 16KHz sampling standards such as AAC.
- It shall support audio modes such as - OFF or Mic (Line) input or Audio output or Interactive (Half duplex) or Interactive (Full duplex)
- The camera shall have mini-jack connectors accessible via pigtail to support external microphone and active speakers.

MECHANICAL REQUIREMENTS:

- The camera shall have 360° endless pan rotation and 0° to 180° tilt range. The unit shall be designed for ceiling mount operation.
- The camera shall have maximum pan/tilt speeds of 350° per second in presets.
- The camera shall have onehundred (100) user defined presets.
- The camera shall be vandal resistant with IK10 rating or IEC 62262 compliance.
- The camera shall have inbuilt dehumidification/defog feature to remove moisture from the camera.
- The camera shall be outdoor rated having IP66 rating for ingress protection.

3.3. FULL HIGH DEFINITION, TRUE DAY/NIGHT, MINIDOME NETWORK CAMERA (3-8mm)

GENERAL REQUIREMENTS:

- The camera shall be a Full HD dome network camera supporting three codecs, JPEG/MJPEG and 2 nos. H.264 high profile, any two of which can be used simultaneously. The camera shall utilize a 1/3" type CCD/MOS/CMOS sensor of approx. 2.0 Megapixels and have a true day/night capability.
- The camera shall be ONVIF Profile S compliant.
- The camera shall have an IK10 rated vandal-proof housing and shall comply with IEC 62262, IEC 60068-2-75 test standard for impact resistance.
- The camera shall support JPEG/MJPEG format and H.264 high profile compression. The camera shall be able to select the high quality mode in JPEG/MJPEG 1920x 1080 at minimum 25fps. The camera shall also be able to support full HD mode of 1920 x 1080 in H.264 compression mode with 30fps.
- The camera shall provide minimum 3 streams, namely, 1 x JPEG/MJPEG and 2 x H.264 High Profile.
- The camera shall incorporate a built-in web server, so that a standard web browser such as Microsoft Internet Explorer, Mozilla Firefox or Google Chrome can be used to access the camera without need for special viewer software.
- The camera shall have an advanced function which will allow the camera image to be viewed in JPEG format without using any plug-ins and thus allowing HTML code for the video image to be generated, allowing for easy web page integration.
- The camera shall be capable of supporting up to five (05) users simultaneously over the network.
- The camera shall have light control mode to select the operating environment, i.e., indoor or outdoor.
- The camera shall have a 2D and 3D noise reduction capability for reducing AGC noise to provide clear images without motion blur.
- The network interface shall be an 8-pin RJ-45 connector, 10Base-T/100Base-TX Ethernet. Both IPv6 and IPv4 shall be supported.
- The camera shall have built-in motion detection capability.
- The camera shall support the following Network protocols: TCP/IP, UDP/IP, HTTP, RTSP, RTP, RTP/RTCP, FTP, SMTP, DHCP, DNS, DDNS, NTP, and SNMP.
- The camera shall support HTTPS client authentication.
- The camera shall have user configurable port settings.
- The camera shall have an integral 3 to 9 mm p-iris type vari-focal lens with remote zoom and focus.
- The camera shall be Power over Ethernet (PoE) capable, compliant to the IEEE 802.3af standard.
- The camera shall have privacy zone masking for blocking out unwanted or prohibited areas within the video image to protect privacy.

- The camera software should include IP Setup (including group camera management) program, Firmware Upgrade Tool, Privacy Masking Tool. The software shall be supplied with the camera as a standard accessory.
- The minimum electronic shutter setting shall be 1 second, and a maximum of 1/40,000 sec.
- The camera shall be capable of limiting the bandwidth from 64 kbps to 8 Mbps in MPEG-4 or H.264 high profile, and from 0.5 Mbps to an unlimited bandwidth in JPEG.
- The camera shall be capable of automatically transmitting alarm images transfer via FTP file transfer and/or e-mail. In addition the network camera shall support scheduled transfer of image information via FTP to an FTP server.
- The camera shall feature a body-based automatic back focus mechanism for automatic and remote back focus adjustment by way of hardware button or software based control.

CAMERA LENS SPECIFICATIONS:

- Focal length shall be 3 to 8 mm with field of view coverage of approximately 90° to 34°

VIDEO-ELECTRICAL REQUIREMENTS:

- The camera input power shall be PoE 802.3af compliant source.
- The camera shall operate at a minimum scene illumination of: 0.3 lux in colour and 0.065 lux in B/W mode, 0 lux with IR.
- The IR range shall be upto 20 mtrs
- The camera shall have multiple ON/OFF/Selectable AGC levels which can be set from the settings menu.

MECHANICAL REQUIREMENTS:

- The camera shall have compliance to IEC 60529 standard. Also, it shall have IK10 rated vandal resistant body for reliability.

3.4. FULL HIGH DEFINITION, OUTDOOR FIXED CS-MOUNT/BOX CAMERA**GENERAL REQUIREMENTS:**

- The camera shall be a Full HD fixed-type CS-mount network camera supporting three codecs – 1 x JPEG/MJPEG and 2 x H.264 high profile streams. Camera shall have a 1/3" type CMOS/MOS sensor and have a resolution of approx. 2.0 MP and have a True day/night capability.
- The camera shall be ONVIF Profile S compliant.
- The camera shall support JPEG/MJPEG and H.264 high profile compression. The camera shall be able to select the high quality mode in JPEG 1920 x 1080 at minimum 25fps. The camera shall also be able to support full HD mode of 1920X1080 in H.264 compression mode with 30fps. The camera shall support JPEG and H.264 high profile compression
- The network interface shall be an 8-pin RJ-45 connector, 10Base-T/100Base-TX Ethernet. Both IPv6 and IPv4 shall be supported.
- The camera shall incorporate a built-in web server, so that a standard web browser such as Microsoft Internet Explorer, Mozilla Firefox or Google Chrome can be used to access the camera without need for special viewer software.

- The camera shall be capable of supporting up to five (05) users simultaneously over the network.
- The camera shall have built-in motion detection capability.
- The camera shall support the following Network protocols: TCP/IP, UDP/IP, HTTP, HTTPS, RTSP, RTP, RTP/RTCP, FTP, SMTP, DHCP, DNS, DDNS, NTP, SNMP, UPnP, IGMP, ICMP, ARP
- The camera shall have both FTP client and server capabilities.
- The camera shall have user configurable port settings.
- The camera shall have a CS-mount 2MP IR corrected type 5-50mm vari-focal lens.
- The camera shall be Power over Ethernet capable, compliant to the 802.3af standard.
- The camera shall have privacy zone masking for blocking out unwanted or prohibited areas within the video image to protect privacy.
- The camera shall have the capability for Camera ID as well as Date/Time data to be superimposed on the video image.
- The camera shall have light control mode to select the operating environment, i.e., indoor or outdoor.
- The camera shall have a 2D and 3D noise reduction capability for reducing AGC noise to provide clear images without motion blur.
- The camera shall be capable of automatically transmitting alarm images transfer via FTP file transfer and/or e-mail. In addition the network camera shall support scheduled transfer of image information via FTP to an FTP server.
- The minimum electronic shutter setting shall be 1second, and a maximum of 1/40,000 sec.
- The camera shall be capable limiting the bandwidth from 64 kbps to 8192 kbps in H.264 high profile and an unlimited bandwidth in JPEG.
- The camera shall support multi-casting and unicasting

CAMERA LENS SPECIFICATIONS

- The camera shall have a CS-mount DC auto-iris type vari-focal lens - Focal length shall be 5-50mm.
- The aperture range for the lens shall be F1.2 to F1.9.

VIDEO- ELECTRICAL REQUIREMENTS

- The camera input power shall be PoE 802.3af compliant source.
- The camera shall operate at a minimum scene illumination of: 0.3 lux in colour and 0.06 lux in B/W mode.
- The camera shall have multiple ON/OFF/Selectable AGC levels which can be set from the settings menu.

MECHANICAL REQUIREMENTS

- The camera shall have a CS type camera lens mount.

- The camera lens supplied with the camera shall be IR corrected lens supplied by the camera OEM or other reputed makes of lens such as Tamaron or Fujinon or equivalent and having focal length 5-50mm, F1.2 to F1.9, DC auto-iris type vari-focal lens.
- The camera shall be installed in a vandal resistant IK10 rated housing.
- The camera shall be outdoor rated and having IP66 rating for ingress protection.

3.5. FULL HIGH DEFINITION, INDOOR FIXED CS-MOUNT/BOX CAMERA

GENERAL REQUIREMENTS:

- The camera shall be a Full HD fixed-type CS-mount network camera supporting three codecs – 1 x JPEG/MJPEG and 2 x H.264 high profile streams. Camera shall have a 1/3" type CMOS/MOS sensor and have a resolution of approx. 2.0 MP and have a True day/night capability.
- The camera shall be ONVIF Profile S compliant.
- The camera shall support JPEG/MJPEG and H.264 high profile compression. The camera shall be able to select the high quality mode in JPEG/MJPEG 1920 x 1080 at minimum 25fps. The camera shall also be able to support full HD mode of 1920X1080 in H.264 compression mode with 30fps.
- The network interface shall be an 8-pin RJ-45 connector, 10Base-T/100Base-TX Ethernet. Both IPv6 and IPv4 shall be supported.
- The camera shall incorporate a built-in web server, so that a standard web browser such as Microsoft Internet Explorer, Mozilla Firefox or Google Chrome can be used to access the camera without need for special viewer software.
- The camera shall be capable of supporting up to five (05) users simultaneously over the network.
- The camera shall have built-in motion detection capability.
- The camera shall support the following Network protocols: TCP/IP, UDP/IP, HTTP, HTTPS, RTSP, RTP, RTP/RTCP, FTP, SMTP, DHCP, DNS, DDNS, NTP, SNMP, UPnP, IGMP, ICMP, ARP
- The camera shall have both FTP client and server capabilities.
- The camera shall have user configurable port settings.
- The camera shall have a CS-mount 2MP IR corrected type vari-focal lens 3-8 mm as standard accessory.
- The camera shall be Power over Ethernet capable, compliant to the 802.3af standard.
- The camera shall have privacy zone masking for blocking out unwanted or prohibited areas within the video image to protect privacy.
- The camera shall have the capability for Camera ID as well as Date/Time data to be superimposed on the video image.
- The camera shall have light control mode to select the operating environment, i.e., indoor or outdoor.
- The camera shall have a 2D and 3D noise reduction capability for reducing AGC noise to provide clear images without motion blur.
- The camera shall be capable of automatically transmitting alarm images transfer via FTP file transfer and/or e-mail. In addition the network camera shall support scheduled transfer of image information via FTP to an FTP server.

- The minimum electronic shutter setting shall be 1 second, and a maximum of 1/40,000 sec.
- The camera shall be capable limiting the bandwidth from 64 kbps to 8192 kbps in H.264 high profile and an unlimited bandwidth in JPEG.
- The camera shall support multi-casting and unicasting.

CAMERA LENS SPECIFICATIONS

- The camera shall have a CS-mount DC auto-iris type vari-focal lens - focal length shall be 3-8mm.
- The aperture range for the lens shall be F1.2 to F1.9.

VIDEO- ELECTRICAL REQUIREMENTS

- The camera input power shall be PoE 802.3af compliant source.
- The camera shall operate at a minimum scene illumination of: 0.3 lux in colour and 0.06 lux in B/W mode.
- The camera shall have multiple ON/OFF/Selectable AGC levels which can be set from the settings menu.

MECHANICAL REQUIREMENTS

- The camera shall have a CS type camera lens mount.
- The camera lens supplied with the camera shall be IR corrected lens supplied by the camera OEM or other reputed makes of lens such as Tamaron or Fujinon or equivalent and having focal length 3-8mm, F1.2 to F1.9, DC auto-iris type vari-focal lens.
- The camera shall be installed in a vandal resistant IK10 rated housing.

3.6. VIDEO MANAGEMENT SOFTWARE (VMS)

- The application must be able to support multiple brands of surveillance cameras at the same time.
- In order to ensure an openness of the system the VMS application provider shall be different than the camera make.
- The VMS shall support SDK (Software Development Kit) integration for integrating third party systems.
- The VMS shall support ONVIF or PSI alliance – industry standards for the interface of IP-based physical security products.
- The VMS shall allow the direct configuration of IP camera device with no requirement to directly connect via web page of IP camera or encoder to configure parameters such as Discovery on IP network and set IP Address, Frame Rate, Resolution, Motion Detection (within camera or server based), Bit Rate, Key frame interval, Digital I/O, Audio Inputs/Outputs, Ability to update firmware of IP camera or encoder. Any configuration changes do not require these services to be restarted.
- The VMS shall be compatible with both 32-bit and 64-bit operating systems including clients working on Windows 7 or later and server operating systems version Windows Server 2003/2008 or later.
- The VMS shall be based on a true open architecture that shall allow for use of non-proprietary workstation and server hardware, non-proprietary network infrastructure and non-proprietary storage.
- The VMS shall offer a complete and scalable video surveillance solution which allows cameras to be added on a unit-by-unit basis.
- All video streams supplied from analog cameras or IP cameras shall be digitally encoded in H.264 or better compression formats and recorded simultaneously in real time.
- The VMS shall support configuration of individually configurable multiple streams for Live & Recording. This functionality shall also support configuration of each camera stream separately. Altering the setting of one camera shall not affect the recording & display settings of other cameras.
- The VMS shall be able to use multiple CCTV keyboards to operate the entire set of cameras throughout the system, including cameras of various manufacturers' brands, including their PTZ functionalities.
- The VMS shall be able to retrieve and set the current position of PTZ cameras with presets.
- The VMS shall consist of a role-based architecture, with each server hosting one or more roles, typical roles or functions such as the following:
- The system shall be managed by a Central Database Role that would contain all the system information and component configuration.
- Database Management Role to authenticate users and give access to the system based on predefined user access rights or privileges, security partition settings, configuration of camera units, access control units, PTZ functionalities, camera sequences and recording schedules.

- Video Recording Role for managing cameras and encoders under its control and archiving video.
- Routing Role for routing video and audio streams across the networks from the source to destination.
- Health Monitoring Role for monitoring and logging health events and warnings from the various client applications, roles, and services. It shall also log events within the Windows Event Log, generating reports on health statistics and health history.
- Surveillance User Interface shall be provided for monitoring of video from the cameras, transactions from access control and the events & alarms. The interface shall also facilitate recording of the video.
- A User Interface for controlling of Pan Tilt & Zoom functionality and pre-sets of PTZ cameras besides other functions such as - control of iris and focus of the camera, perform digital zooming on the live as well as playback video.
- The User Interface shall allow administrators and operators with appropriate privileges to monitor the VMS system, run reports, and manage alarms.
- The User Interface shall support following to enhance usability and operator efficiency such as:
 - Use of transparent overlays that can display multiple data in a seamless fashion.
 - Display tile menus and quick commands.
 - Consolidated and consistent workflows.
 - Tile menus and quick commands easily accessible within every display tile of the user workspace.
- The User Interface shall have task for investigation of video bookmark, smart motion search, archive reports, audit trails and activity reporting.
- The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to limit what users and operators can modify in their work space through privileges.
- Once customized, the user shall be able to save his/her workspace.
- The user workspace shall be accessible by a specific user from any client application on the network.
- Display tile patterns shall be customizable.
- Facility shall be available for event or alarm lists to be displayed on any part of the screen, from a portion of the screen up-to the entire screen, and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.
- The User Interface shall support multiple display tile patterns,e.g., 1 display tile(1x1 matrix),16tiles(8x8matrix)and multiple additional variations.
- The User Interface shall support as many monitors as the PC video adapters and Windows Operating System are capable of accepting.
- Shall support live video monitoring on each and every display tile within a task in the user's workspace.

- The operator shall be able to drag and drop a camera into a display tile for live viewing.
- The operator shall be able to start/stop recording on any camera in the system, which is configured to allow manual recording, by clicking on a single button.
- The operator shall be able to switch one or more video tile to switch for instant replay. This operation shall not affect live monitoring of other cameras.
- Users shall be able to take snapshots of live video and be able to save or print the snapshots.
- The user shall be able to view the same camera multiple times in different tiles.
- A Server Monitoring Service shall be installed on all PCs/servers running with VMS platform. In the event of a malfunction or failure, the Server Monitoring Service shall restart the failed service. As a last resort, the Server Monitoring Service shall reboot the server/PC if it is unable to restart the service.
- The platform shall support the Alarm Management functionality. The User shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze. The user shall able to spontaneously trigger alarms based on something he or she sees in the system.
- The Surveillance User interface's video playback capabilities shall include:
 - Audio and video play back of any time span.
 - Video play back on each and every display tile.
 - Allowing operators to switch to instant replay of the video for any archiving camera with the simple click of button.
 - Allowing the operator to select between instant synch of all video streams in play back mode allowing operators to view events from multiple angles or across several camera fields, or non-synchronous playback.
 - Allowing the operator to simultaneously view the same camera in multiple tiles at different time intervals.
 - Allowing the operator to control the play back with:
 - Pause
 - Lock Speed
 - Forward and Reverse
Playback at: 1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x (at least up to 40x)
 - Forward and Reverse Play back frame by frame
 - Slow Forward and Reverse Playback at: 1x/8x, 1/4x, 1/3x, 1/2x.
 - Loop play back between two time markers
 - Displaying a single timeline, or optionally one timeline for each selected video stream, with which the operator can navigate through the video sequence by simply clicking on any point in the timeline.
 - Displaying the level of motion at any point on a timeline.
 - Allowing to query archived video using various search criteria, including but not limited to, time, date, camera, and area, among others.

- Providing a tool to search video and associated audio on user-defined events or motion parameters.
- Allowing operators to define an area of the video field in which to search for motion as well as define the amount of motion that shall trigger search results in order to retrieve all archived video streams which contain motion which meets the search parameters. There shall be a graphical timeline where the time of each search hit shall be indicated.
- Supporting digital zoom on play back video streams.
- Providing still image export to PNG, JPEG, GIF, and BMP format with Date and Time stamp and Camera Name on the image (snapshot).
- Providing tools to export video on various media such as a DVD.
- Allowing operators to load previously exported video files from their computer or network.
- The VMS shall permit the user to select multiple entities to be monitored from the Surveillance User Interface.
- The User Interface shall support the ability to manually track a moving target with the single click of a button.
- Visual tracking shall be available with both live and recorded video.
- The user interface monitoring client shall able to take control of other client station based on the privilege level and control the tile of the other client like a video wall application.

CONFIGURATION USER INTERFACE

- The Configuration User Interface shall allow the administrator or users with appropriate privileges to change video configuration.
- It shall provide the ability to change video quality, bandwidth and frame rate parameters on a per camera (stream) basis for both live and recorded video.
- It shall provide the ability to configure brightness, contrast and hue settings for each camera on the same.
- The Configuration user interface shall provide the capability to enable & change audio parameters, audio recording serial port configuration, I/O configuration on camera device units.
- The Configuration User Interface shall provide the ability to set recording schedules and modes for each individual camera, e.g.,:
 - Continuous
 - On motion and Manual
 - Manual only
 - Disabled
- The Configuration User Interface shall support the creation of schedules to which any of the following functional aspects can be attached:
 - Video quality(for each video stream per camera)
 - Recording(for each camera)

- Motion detection(for each detection zone per camera)
- Brightness, Contrast, Hue(for each camera)
- Camera sequence execution
- The configuration User Interface shall support creation of unlimited recording schedules and assign any camera to any schedules.
- The Configuration User Interface shall provide the capability to set a pan-tilt-zoom protocol to a specific camera device serial port and allow mixing domes of various manufacturers within a system.

ARCHIVING

- The Archiver (Recording role) shall use an event and time stamp database for advanced search of audio/video archives. This database shall be Microsoft SQL 2008 or SQL 2012 or later
- The Archiver shall digitally sign the recorded video.
- The Archiver shall offer a plug and play type hardware discovery service with the following functionalities:
- The Archiver shall have the capacity to configure the key frame interval in seconds or number of frames.
- The Archiver shall support configuration of pre-alarm and post-alarm recording option that can be set between one second and 5 minutes on a per camera basis.
- The Archiver shall support minimum 300 cameras or 300 Mbps of recording throughput whichever comes first in case the network is end to end multicast.
- The Archiver shall support software level motion detection.
- Software level motion detection shall be able to divide camera field of view in 5 detection zones for setting up individual motion settings in each zone and trigger an event for each zone separately.
- The Archiver shall be able to communicate with camera using 128bits SSL encryption and HTTPS secure protocol.
- The Archiver shall be able to receive multicast UDP streams directly from the camera.
- For network topologies that restrict the camera from sending multicast UDP streams, the Archiver shall redirect audio/video streams to active viewing clients on the network using multicast UDP.
- The Archiver shall be able to redirect audio/video stream to active viewing clients on the network using unicast UDP or TCP.
- The user interface of the monitoring station shall support dynamically switching the live stream from – High Resolution, Low Resolution & Live (normal).
- The Archiver shall allow configuration of retention period for archiving video for pre-set number of days. It shall also delete oldest video data if the disk is full before the retention time occurs.
- The Archiver shall allow important video sequences to be protected against normal disk clean-up routines.

- The Archiver shall keep a log and compile statistics on disk space usage.
- The Archiver shall have the capacity to down-sample video streams for storage saving purposes.

FAILOVER AND STANDBY FUNCTIONALITY

- The Standby Directory Role shall take over the responsibility of system management in case the primary directory fails. The fail over shall occur in less than 1 minute. No action from the user shall be required.
- This functionality shall be achievable without using the windows clustering.
- The Standby Archiver shall act as replacement of Archiver role on hot standby in case the primary Archiver role is unavailable. Failover shall occur in less than 1 minute. No action from the user shall be required.
- Failover Archiver shall take over for – server failure, storage failure, manually shift the Archiver Role to standby Archiver to perform maintenance activity on primary server.
- It shall be possible for a single Standby Archiver Server to act as the Standby for one or multiple Archiver roles.
- It shall be possible for any Archiver role in the system to be designated as another's stand by and vice-versa.
- The Standby Archiver shall have the ability to act as a Redundant Archiver and maintain an exact copy of everything recorded by the default Archiver, i.e., audio/video archives, events and bookmarks.
- Redundancy shall be configured on a camera by camera basis.
- The Redundant Archiver shall use a multicast video stream from the camera and shall not require an additional connection to any camera.

UNIFIED WEBCLIENT

- Web client shall be supported for video & access control.
- The Web client shall be a thin client with no download required other than an internet web browser or standard web browser plug-ins.
- The Web client shall be platform independent and run within Microsoft Internet Explorer, Firefox, Safari, and Google Chrome.

SMART PHONE AND TABLET APPS

- The VMS shall support mobile apps for various popular smart phones and tablets, including e.g., Apple iOS based devices and Android based devices
- It shall support monitoring of live camera, receive alarm push notifications, save snapshots locally on device or control PTZ.

3.7. VIDEO SURVEILLANCE STORAGE

Configuration & Specification for Storage System for Video Surveillance & Recordings on a 24 Hrs x 30Days Basis**1. High Availability**

- The proposed solution should be a storage system configured with dual, redundant controllers.
- Each controller must have Intel Sandy Bridge Quad core CPU per controller or equivalent.
- The proposed solution should be based on real time optimized operating system and should not be a general purpose OS.
- The proposed solution should support online Microcode / OS upgrades.
- Must provide five 9's availability (99.999%)

2. Investment Protection

- The proposed storage should be non-disruptively upgraded to 10G Ethernet, FC and FCoE protocols in future and managed by the same storage management software.
- Storage system quoted by the OEM should be in the Leaders Quadrant in the latest Gartner Magic Quadrant for Midrange and High End Modular Storage Arrays Report.

3. RAM, Scalability and HDD Support

- The controllers should have a minimum 30GB cache spread across dual controllers.
- The proposed solution should be scalable to more than 110 drives in the same storage array without the need for upgrading the controllers.

4. Host Connectivity and Storage Backend Disk Connectivity

- The offered storage shall be supplied with at least 8nos x 1G iSCSI Ports across dual controllers for host connectivity.
- The array proposed should have a minimum of 4nos x 6Gbps 2.0 SAS backend architecture.

5. Total Aggregate Bandwidth

- The Proposed storage disk should ensure a minimum total aggregate bandwidth of 2500Mbps on a 90% write &10% read application environment.

6. RAID Support

- All RAID types should be industry standard RAID and solution to be configured with RAID5 protection.
- For every 30 disks, 1 no disk should be configured as Global hot spare.

7. Management

- The proposed solution should support a browser based built in management. It should have SNMP support. (Traps, e-mail, MIB II)

8. Current Required Protocols

- The proposed solution must support and be configured for FC &iSCSI protocols.

9. Storage Capacity Requirements

- The proposed storage array should be configured with Minimum 150TB usable capacity using SATA/NL-SAS Drives. The usable capacity is defined as the net storage capacity available for the application stack, after deducting the penalties imposed by storage infrastructure requirements, disk and array formatting, RAID penalties, host OS and file system formatting including overheads or any other penalties which eat away usable disk space. Drives offered for the above capacity shall be of the highest capacity offered by the vendor.
- The same storage system should support 50% extra growth in terms of performance and capacity for future expansion without any controller upgrade.

10. Regulatory Model

- The device should have the following certifications - FCC Class A or CE Mark for immunity against electromagnetic emissions.

11. Safety and Quality Standards

- The device should have the following quality and safety standard certifications - CAN/CSAC22.2-60950/UL60950.

3.8. SERVERS AND CLIENTS FOR VIDEO SURVEILLANCE SYSTEM

- Server Hardware - Industry standard Intel based platform, rack mountable, redundancy architecture for critical hardware components, licensed Microsoft Server Operating system as per VMS OEM and requisite user licenses, licensed application suites, Processor: 2 x Quad Core Intel® Xeon® 5150, 2.66 GHz, 4 MB Cache, 1333 MHz FSB or better or as per CCTV/VMS OEM, min. 8 GB of RAM, 500 GB storage or more, additional hard drive(s) for video storage, 1360 x 768 or higher screen resolution, 10/100/1000 Ethernet Network Interface Card, DVD ROM Drive.
- Client Hardware - Industry standard Intel based platform, rack mountable, licensed Microsoft Operating system and requisite user licenses, licensed application suites. Intel Core i7 2600 @ 3.4 GHz or higher, min. 8 GB RAM DDR3, 500 GB SATA II hard drive for OS and VMS applications, NVidia GTX 570 or DirectX VA 2.0 compatible card with 1 GB of RAM, 1600 x 1200 or higher screen resolution , 10/100/1000 Mbps Ethernet Network Interface Card, min. 16x DVD+/- RW Drive.
- Required Operating Systems:
 - For Client PCs: Microsoft® Windows 10 or higher Professional or Ultimate 32-bit/64-bit
 - For Server:» Microsoft® Windows Server® 2012 Standard Edition 64-bit » Microsoft® Windows Server® 2012 Enterprise Edition 64-bit, or later as per VMS OEM requirements
- Browser Requirements» Internet Explorer 6, 7 or 8 (for Web Clients), latest versions of Mozilla Firefox and Google Chrome

3.9. 5-PORT INDUSTRIAL PoE+ SWITCH WITH 2-PORT POPULATED MINI GBIC SFP PORTS:**Switch Properties:**

1.	MAC table size:	1K
2.	Packet buffer size:	512 kb
3.	Processing Type:	Store and Forward

Interface:

1.	Fiber Ports: LC connector)	2 x 100BaseFX ports (single mode,
2.	RJ45 Ports: speed,	3 x 10/100BaseT(X) auto negotiation Full/Half duplex mode, and auto MDI/MDI-X connection
3.	PoE Pin out:	V, V, V+, V+ for pin 1, 2, 3, 6 (End span, MDI-X Alternative A)
4.	LED Indicators:	PWR1, PWR2, 10/100M, PoE
5.	Alarm Contact:	2 relay outputs with current carrying capacity of 1 A @ 24 VDC

Power Requirements (Unit shall be provided with required power supply)

- | | | |
|----|------------------------------|---|
| 1. | Input Voltage: | 24/48 VDC (20 to 60 VDC),
redundant inputs |
| 2. | Input Current: | Max 7.5 A @ 24 VDC (shall
support up to 4 ports at 30W per Po
E port) |
| 3. | Overload Current Protection: | Yes |
| 4. | Connection: | removable 4-contact terminal blocks |
| 5. | Reverse Polarity Protection: | Yes |

Physical Characteristics

- | | | |
|----|---------------|----------------------------------|
| 1. | Housing: | Metal, IP30 protection |
| 2. | Installation: | DIN-Rail mounting, wall mounting |

Standards

- | | |
|----|---------------------------------------|
| 1. | IEEE 802.3at for Power-over-Ethernet+ |
| 2. | IEEE 802.3 for 10BaseT |
| 3. | IEEE 802.3u for 100BaseT(X) |
| 4. | IEEE 802.3x for Flow Control |

Standards & Certifications

- | | |
|----|-----------------------|
| 1. | UL 508 |
| 2. | UL 60950-1 |
| 3. | CSA C22.2 No. 60950-1 |
| 4. | EN 60950-1 |

Environmental Limits

- | | | |
|----|---------------------------|--|
| 1. | Operating temperature | 0 to 60°C (32 to 140°F) minimum.
And upto-40 to 75°C (-40 to 167°F) |
| 2. | Storage Temperature | -40 to 85°C (-40 to 185°F) |
| 3. | Ambient Relative Humidity | 5 to 95% (non-condensing) |

4. FIRE DETECTION, ALARM AND CONTROL SYSTEM (FAS)

GENERAL SYSTEM DESCRIPTION

- This section of the specification includes the furnishing, installation, connection and testing of the microprocessor controlled, intelligent reporting fire alarm equipment required to form a complete, operative, coordinated system. It shall include, but not be limited to, alarm initiating devices, alarm notification appliances, Fire Alarm Control Panel (FACP), auxiliary control devices, annunciators, and wiring as shown on the drawings and specified herein.
- The fire alarm system shall comply with requirements of NFPA Standard 72(2013), IS 2189(2008) and NBC 2016 for Protected Premises Signalling Systems. The system shall be electrically supervised and monitor the integrity of all conductors.
- The fire alarm system shall be manufactured by an ISO 9001 certified company and meet the requirements of BS EN9001: ANSI/ASQC Q9001-1994
- The system and its components shall be Underwriters Laboratories, Inc. listed under the appropriate UL testing standard for fire alarm applications. It should be FM (Factory Manual) approved and the installation shall be in compliance with the UL listing.
- The panel shall be supplied with all accessories, control modules and power supplies in the required quantities as per site requirements for all types of field devices to make the system fully operational.
- The FAS shall be supplied with necessary hardware and software so as to ensure networking of all panels. This shall include all devices such as modules and interfaces for providing fiber-optics based connectivity between panels and any licences, as applicable.
- The detectors and devices connected to the fire alarm panel's loop(s) shall be auto-addressable via panel or software or manually addressable via a rotary switch or DIP switch.
- The FAS system shall be supplied with all functionality including hardware, software and licences for integration with a third party IBMS system for real-time monitoring, supervision and control. The necessary interfaces and functionality for such networking protocols as BaCNet/IP shall be provided.
- FAS panels shall have facility for at least two levels of password based access – typically such as complete admin rights providing access to all functions (primary or admin or master) and a secondary level access for reading only and accessing logs and reports etc.

SCOPE

- An intelligent reporting, Intelligent addressable microprocessor controlled fire detection system shall be installed in accordance to the project specifications and drawings.
- **Basic Performance:**
 - Alarm, trouble and supervisory signals from all intelligent reporting devices shall be encoded on Class A Signalling Line Circuits (SLC).
 - Initiation Device Circuits (IDC) shall be wired Class A as part of an addressable device connected by the SLC Circuit.
 - Notification Appliance Circuits (NAC) shall be wired Class A as part of an addressable device connected by the SLC Circuit.

- On Class A configurations a single ground fault or open circuit on the system Signalling Line Circuit shall not cause system malfunction, loss of operating power or the ability to report an alarm.
- Alarm signals arriving at the FACP shall not be lost following a primary power failure (or outage) until the alarm signal is processed and recorded.

EQUIPMENT AND MATERIAL, GENERAL:

- All equipment and components shall be new, and the manufacturer's current model. The materials, appliances, equipment and devices shall be tested and listed by a nationally recognized approvals agency for use as part of a protective signalling system, meeting the National Fire Alarm Code.
- All equipment and components shall be installed in strict compliance with manufacturers' recommendations. Consult the manufacturer's installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation.
- All equipment shall be attached to walls and ceiling/floor assemblies and shall be held firmly in place (e.g., detectors shall not be supported solely by suspended ceilings). Fasteners and supports shall be adequate to support the required load.

4.1. MAIN FIRE ALARM CONTROL PANEL OR NETWORK NODE:

- Main FACP or network node shall contain a microprocessor based Central Processing Unit (CPU) and power supply. The CPU shall communicate with and control the following types of equipment used to make up the system: intelligent addressable detectors of various types, addressable modules, printer, annunciators, and other system controlled devices.

CENTRAL MICROPROCESSOR

- The microprocessor shall be a state-of-the-art, high speed, 16-bit RISC device and it shall communicate with, monitor and control all external interfaces. It shall include an EPROM for system program storage, Flash memory for building-specific program storage, and a "watch dog" timer circuit to detect and report microprocessor failure.
- The microprocessor shall contain and execute all control-by-event programs for specific action to be taken if an alarm condition is detected by the system. Control-by-event equations shall be held in non-volatile programmable memory, and shall not be lost even if system primary and secondary power failure occurs.
- The microprocessor shall also provide a real-time clock for time annotation of system displays, printer, and history file. The time-of-day and date shall not be lost if system primary and secondary power supplies fail. The real time clock may also be used to control non-fire functions at programmed time-of-day, day-of-week, and day-of-year.
- A special program check function shall be provided to detect common operator errors.
- An auto-program (self-learn) or a pre-configuration from software function shall be provided to quickly install initial functions and make the system operational.
- For flexibility and to ensure program validity, an optional Windows(TM) based program utility shall be available. This program shall be used to off-line program the system with batch upload/download, and have the ability to upgrade the manufacturers (FLASH) system code changes. This program shall also have a verification utility, which scans the program files, identifying possible errors. It shall also have the ability to compare old program files to new ones, identifying differences in the two files to allow complete testing of any system operating changes. This shall be in compliance with the NFPA 72 requirements for testing after system modification.

OPERATOR CONTROL**1. Acknowledge Switch:**

- Activation of the control panel acknowledge switch in response to new alarms and/or troubles shall silence the local panel piezo electric signal and change the alarm and trouble LEDs from flashing mode to steady-ON mode. If multiple alarm or trouble conditions exist, depression of this switch shall advance the LCD display to the next alarm or trouble condition.
- Depression of the Acknowledge switch shall also silence all remote annunciator piezo sounders.

2. Alarm Silence Switch:

- Activation of the alarm silence switch shall cause all programmed alarm notification appliances and relays to return to the normal condition after an alarm condition. The selection of notification circuits and relays that are silence-able by this switch shall be fully field programmable within the confines of all applicable standards. The FACP software shall include silence inhibit and auto-silence timers.

3. Alarm Activate (Drill) Switch:

- The Alarm Activate switch shall activate all notification appliance circuits. The drill function shall latch until the panel is silenced or reset.

4. System Reset Switch:

- Activation of the System Reset switch shall cause all electronically-latched initiating devices, appliances or software zones, as well as all associated output devices and circuits, to return to their normal condition.

5. Lamp Test:

- The Lamp Test switch shall activate all local system LEDs, light each segment of the liquid crystal display and display the panel software revision for service personal.

4.2. SYSTEM CAPACITY AND GENERAL OPERATION**SIGNALING LINE CIRCUITS (SLC)**

- Each loop of the fire alarm panel shall provide power to and communicate with up to a minimum of 127 intelligent addressable detectors and 127 intelligent addressable modules (monitor or control) or a mix of up to 250 detectors and devices in any combination.
- Type 1: The control panel or each network node shall be equipped with 1 installed loop with each loop having a capacity of a minimum 127 addressable detectors and 127 addressable modules or a mix of up to 250 detectors and devices in any combination with max. 80% of loop loading in a single loop. It shall be modularly expandable up to minimum 10 loop capacity with each loop having a capacity of minimum 127 addressable detectors and 127 addressable modules or a mix of up to 250 detectors and devices in any combination with max. 80% of loop loading in a single loop. However, the number of loop cards can be done as per the OEM configuration.
- Type 2: The control panel or each network node shall be equipped with 2 installed loops with each loop having a capacity of a minimum 127 addressable detectors and 127 addressable modules or a mix of up to 250 detectors and devices in any combination with max. 80% of loop loading in a single loop. It shall be modularly expandable up to minimum 10 loop capacity with each loop having a capacity of minimum 127 addressable detectors and 127 addressable modules or a mix of up to 250 detectors and devices in any combination with max. 80% of loop loading in a single loop. However, the number of loop cards can be done as per the OEM configuration.

- Type 3: The control panel or each network node shall be equipped with 3 installed loops with each loop having a capacity of a minimum 127 addressable detectors and 127 addressable modules or a mix of up to 250 detectors and devices in any combination with max. 80% of loop loading in a single loop. It shall be modularly expandable up to minimum 10 loop capacity with each loop having a capacity of minimum 127 addressable detectors and 127 addressable modules or a mix of up to 250 detectors and devices in any combination with max. 80% of loop loading in a single loop. However, the number of loop cards can be done as per the OEM configuration.
- Class A (NFPA Style 6) type cabling structure.
- The FACP or each network node shall provide the following features:
 - Drift compensation to extend detector accuracy over life. Drift compensation shall also include a smoothing feature, allowing transient noise signals to be filtered out.
 - Detector sensitivity test, meeting requirements of NFPA 72
 - Maintenance alert, with two levels (maintenance alert/maintenance urgent), to warn of excessive smoke detector dirt or dust accumulation.
 - Detectors shall be programmable as application specific, selected in software for a minimum of eleven environmental fire profiles unique to the installed location. These fire profiles shall eliminate the possibility of false indications caused by dust, moisture, RFI/EMI, chemical fumes and air movement while factoring in conditions of ambient temperature rise, obscuration rate changes and hot/cold smoke phenomenon into the alarm decision to give the earliest possible real alarm condition report.
 - The ability to display or print system reports.
 - Alarm verification, with counters and a trouble indication to alert maintenance personnel when a detector enters verification 20 times.
 - Positive Alarm Sequence - PAS pre signal, meeting NFPA 72 3-8.3 requirements.
 - Rapid manual station reporting (less than 3 seconds) and shall meet NFPA 72 requirements for activation of notification circuits within 10 seconds of initiating device activation.
 - Periodic detector test, conducted automatically by the software.
 - Self optimizing pre-alarm for advanced fire warning, which allows each detector to learn its particular environment and set its prealarm level to just above normal peaks.
 - Cross zoning with the capability of counting: two detectors in alarm, two software zones in alarm, or one smoke detector and one thermal detector.
 - Walk test, with a check for two detectors set to same address.
 - Control-by-time for non-fire operations, with holiday schedules.
 - Day/night automatic adjustment of detector sensitivity.
 - Device blink control for sleeping areas.

4.3. SYSTEM DISPLAY

- The system shall be supplied with a LCD display or a VGA colour LCD display with touch screen.
- The system shall include a full featured operator interface control and annunciation panel that shall include a backlit Liquid Crystal Display (LCD) or a VGA colour LCD display with touch screen, individual colour coded system status LEDs, and an alphanumeric keypad for the field programming and control of the fire alarm system.
- The display shall provide all the controls and indicators used by the system operator such as ACKNOWLEDGE, ALARM SILENCE, ALARM ACTIVATE (drill), SYSTEM RESET, and LAMP TEST.
- The display shall annunciate status information and custom alphanumeric labels for all intelligent detectors, addressable modules, internal panel circuits, and software zones.
- The LCD display or VGA colour LCD display with touch screen shall provide Light-Emitting-Diodes (LEDs) that indicate the status of the following system parameters: AC POWER, FIRE ALARM, PREALARM WARNING, SECURITY ALARM, SUPERVISORY EVENT, SYSTEM TROUBLE, ALARM SILENCED, DISABLED POINTS, OTHER EVENTS, CPU FAILURE and Controls Active.
- The LCD display or VGA colour LCD display with touch screen shall provide a set of "soft" keys for screen navigation or to accomplish dedicated programming functions. Full programming access shall require use of a laptop and the proper programming utility.

4.4. NETWORKCOMMUNICATION AND INTERFACES

- The FACP shall be capable of communicating with each other on a Local Area Network (LAN) over dedicated 12 core single mode fiber optic cable connectivity, utilizing a peer-to-peer protocol.
- The system shall include min. two serial EIA-232 interfaces. Each interface shall be a means of connecting respected certifications or standards (UL/FM).
- Besides, the system shall include interfaces for connecting devices such as printers, LAN interface, RS485, Fiber Optics based connectivity interface, BacNet/IP and Modbus/IP for 3rd party communication.
- The system shall be capable to integrate with ELV and other 3rd party services like Public Address system, Lifts, HVAC, Electric panel etc.

4.5. ENCLOSURES:

- The control panel shall be housed in a standardized cabinet suitable for surface or semi-flush mounting. The cabinet and front shall be corrosion protected, given a rust-resistant prime coat, and manufacturer's standard finish.
- The door shall provide a key lock and shall include a glass or other transparent opening for viewing of all indicators. For convenience, the door may be site configured for either right or left hand hinging.

4.6. POWER SUPPLY:

- An off-line switching power supply shall be available for the fire alarm control panel or network node and provide 6.0 amps of available power for the control panel and peripheral devices.
- Provisions will be made to allow the audio-visual power to be increased as required by adding modular expansion audio-visual power supplies.
- Positive-Temperature-Coefficient (PTC) thermistors, circuit breakers, or other over-current protection shall be provided on all power outputs. The power supply shall have an integral battery charger for use alongwith batteries. The power supply shall continuously monitor all field wires for earth ground conditions, and shall have the following LED indicators:

Ground Fault LED
AC Power Fail LED

- The main power supply shall operate on 230 VAC, 50Hz and shall provide all necessary power for the FACP.
- The main power supply shall provide a battery charger using dual-rate charging techniques for fast battery recharge and be capable of charging batteries up to 100 AH.
- System shall be proposed with backup power from UPS and also independent power backup through Sealed Maintenance Free (SMF) Lead acid Batteries with backup of 24 hours under Normal working condition & 30 minutes under emergency condition of operation under alarm condition with adequate spare capacity overhead.
- The system shall be provided with requisite power supplies, including additional power supplies for the operation of devices such as sounders.

4.7. SYSTEM COMPONENTS - ADDRESSABLE DEVICES

ADDRESSABLE DEVICES - GENERAL

- Addressable devices shall use simple to install and maintain decade, decimal address switches.
- Detectors shall connect with two wires to the fire alarm control panel signalling Line Circuits.
- The fire alarm control panel shall permit detector sensitivity adjustment through field programming of the system. The panel on a time-of-day basis shall automatically adjust sensitivity.
- Detectors shall automatically compensate for dust accumulation and other slow environmental changes that may affect their performance.
- The detectors shall be ceiling-mount and shall include a separate twist-lock base with tamper proof feature. Bases shall include a sounder base with a built-in (local) sounder rated at 85 DBA minimum, a relay base and an isolator base designed for Style 6/7 applications.
- Addressable devices shall store an internal identifying code that the control panel shall use to identify the type of device.
- Addressable modules shall mount in a 4-inch square (101.6 mm square), 2-1/8 inch (54 mm) deep electrical box.

INTELLIGENT MULTI SENSING DETECTOR

- The intelligent multi-sensing detector shall be an addressable device that is designed to monitor a minimum of photoelectric and thermal technologies in a single sensing device. The design shall include the ability to adapt to its environment by utilizing a built-in microprocessor to determine its environment and choose the appropriate sensing settings. The detector design shall allow a wide sensitivity window, no less than 1 to 4% per foot obscuration. This detector shall utilize advanced electronics that react to slow smouldering fires and thermal properties all within a single sensing device.
- The microprocessor design shall be capable of selecting the appropriate sensitivity levels based on the environment type it is in (office, manufacturing, kitchen etc.) and then have the ability to automatically change the setting as the environment changes (as walls are moved or as the occupancy changes).
- The addressable multi-sensing detector shall be capable to configure and to be addressed manually as well as from software or remote locations also.

INTELLIGENT THERMAL OR HEAT DETECTORS

- Thermal detectors shall be intelligent addressable devices rated at 135 degrees Fahrenheit (58 degrees Celsius) and have a rate-of-rise element rated at 15 degrees F (9.4 degrees C) per minute. It shall connect via two wires to the fire alarm control panel signalling line circuit.
- The detector shall be capable to configure and to be addressed manually as well as from software or remote locations also.

BEAM SMOKE DETECTORS

- Sensing Range: 5 to 50 meters
- Adjustment Angle: $\pm 10^\circ$ horizontal and vertical.
- Typical sensitivity levels:
 - Level 1 — 25%.
 - Level 2 — 30%.
 - Level 3 — 40%.
 - Level 4 — 50%.
- Fault Condition (trouble):
 - 96% or more obscuration blockage.
 - In alignment mode.
 - Improper initial alignment.
 - Self-compensation limit reached.
- Alignment Aid using optical gun sight or integral signal strength indication or Two-digit display.

ADDRESSABLE MANUAL CALL BOX

- Addressable manual fire alarm boxes shall on command from the control panel, send data to the panel representing the state of the manual switch and the addressable communication module status. They shall use a key operated test-reset lock, and shall be designed so that after actual emergency operation, they cannot be restored to normal use except by the use of a key.
- All operated stations shall have a positive, visual indication of operation and utilize a key type reset.
- All entrances and stair levels shall be equipped with a pull type manual call point to activate an alarm. Manual call points shall be located in a manner so as to give an easy access to occupants in emergency; these shall be at entry/exits and within 30 meters distance.

SOUNDER AND STROBE:

- Shall follow NFPA 72 2013.
-
- Electronic sounders shall operate on 24 VDC nominal.
- Electronic sounders shall be field programmable without the use of special tools, at a sound level of at least 90 dBA measured at 3 meters from the device.
- Shall be capable to broadcast pre programmed Voice Message also
- Shall be flush or surface mounted as shown on plans.

- Shall produce broad band directional sound with 20 Hz to 20 KHz frequency band to guide occupants to safe exists even in complete darkness.
- Strobe lights shall meet the requirements of the ADA, be fully synchronized, and shall meet the following criteria:
- The maximum pulse duration shall be 2/10 of one second.
- The flash rate shall be minimum 1 flash per second.
- Field Wiring Terminal Blocks
- For ease of service all panel I/O wiring terminal blocks shall be removable, plug-in types and have sufficient capacity for #18 to #12 AWG wire. Terminal blocks that are permanently fixed are not acceptable.

ADDRESSABLE RELAY MODULE

- Addressable Relay Module shall provide a dry potential contact o/p for activating a variety of auxiliary devices and other services equipment (i.e. Smoke Exhaust Fans, Fire Dampers, Access control doors, elevators, PA equipment and HVAC electrical panel such as for AHUs).
- It shall have a various current handling capability of 1A/2A/3A (as required) @ 30 VDC to integrate with third party system.

ADDRESSABLE CONTROL MODULE (WHETHER APPLICABLE SEPERATELY)

- Addressable control modules shall be provided to supervise and control the operation of one conventional NACs of compatible, 24 VDC powered polarized audio/visual notification appliances.
- Audio/visual power shall be provided by a separate supervised power circuit from the main fire alarm control panel or from a supervised remote power supply from the same OEM.
- The control module shall be suitable for pilot duty applications and rated for a minimum of 2.0 amps at 24 VDC.

ISOLATOR MODULE (WHETHER APPLICABLE SEPERATELY)

Isolator modules shall be provided to automatically isolate wire-to-wire short circuits on an SLC Class A or branch. The isolator module shall limit the number of modules or detectors that may be rendered inoperative by a short circuit fault on the SLC loop segment or branch. Each loop shall have isolator module after every 20 detectors to protected zone of the building.

- If a wire-to-wire short occurs, the isolator module shall automatically open-circuit (disconnect) the SLC. When the short circuit condition is corrected, the isolator module shall automatically reconnect the isolated section.
- The isolator module shall not require address-setting, and its operations shall be totally automatic. It shall not be necessary to replace or reset an isolator module after its normal operation.
- The isolator module shall provide a single LED that shall flash to indicate that the isolator is operational and shall illuminate steadily to indicate that a short circuit condition has been detected and isolated.

MONITOR MODULE

- Nominal operating voltage: 15 to 32 VDC.
- Maximum current draw: 5.0 mA (LED on).

- Average operating current: 350 mA (LED flashing, once every 5 seconds)
- Maximum IDC wiring resistance: 40 ohms.
- EOL resistance: 47K ohms.

RESPONSE INDICATOR

- Remote Response Indicator shall be installed outside the areas normally kept closed to identify the detectors response even if the room is locked. These indicators shall be able to indicate the status of the corresponding detectors in these areas.

FIREFIGHTER TELEPHONE JACK AND HANDSET

- Fire-fighter telephone jack is semi-flush mounted receiving plate with a single-gang box. The plate has a single phone jack mounted on an attractive, single-gang, stainless steel plate. Color coded wires, approx. 6 inches long, are prewired to the jack to enable fast and accurate wiring to the system
- Fire-fighter telephone handset comes with a coiled cord. The attached plug fits Fireman's Phone Jack and it is allowing fire-fighters to make direct communication with a central control area

4.8. SYSTEM OPERATIONS

BASIC SYSTEM FUNCTIONAL OPERATION

When a fire alarm condition is detected and reported by one of the system initiating devices, the following functions shall immediately occur:

- The system alarm LED on the system display shall flash.
- A local piezo electric signal in the control panel shall sound.
- A backlit LCD display shall indicate all information associated with the fire alarm condition, including the type of alarm point and its location within the protected premises.
- Printing and history storage equipment shall log the information associated each new fire alarm control panel condition, along with time and date of occurrence.
- All system output programs assigned via control-by-event interlock programming to be activated by the particular point in alarm shall be executed, and the associated system outputs (notification appliances and/or relays) shall be activated.

SPECIFIC SYSTEM OPERATIONS

- Smoke Detector Sensitivity Adjust: A means shall be provided for adjusting the sensitivity of any or all addressable intelligent detectors in the system from the system keypad. Sensitivity range shall be within the allowed standard window and have a minimum of 11 application specific sensitivity levels.
- Alarm Verification: Each of the intelligent addressable smoke detectors in the system may be independently selected and enabled to be an alarm verified detector. The alarm verification delay shall be programmable from 5 to 30 seconds and each detector shall be able to be selected for verification. The FACP shall keep a count of the number of times that each detector has entered the verification cycle. These counters may be displayed and reset by the proper operator commands.
- Point Disable: Any addressable device or conventional circuit in the system may be enabled or disabled through the system keypad.

- Point Read: The system shall be able to display or print the following point status diagnostic functions:
 - a. Device status
 - b. Device type
 - c. Custom device label
 - d. View analog detector values
 - e. Device zone assignments
 - f. All program parameters
- System Status Reports: Upon command from an operator of the system, a status report will be generated and printed, listing all system status.
- System History Recording and Reporting: The fire alarm control panel shall contain an events buffer that will be capable of storing a minimum of 5000 events. Up-to 1000 events shall be dedicated to alarm and the remaining events are general purpose. Each of these activations will be stored and time and date stamped with the actual time of the activation. The contents of the history buffer may be manually reviewed, one event at a time, or printed in its entirety. The history buffer shall use non-volatile memory. Systems that use volatile memory for history storage are not acceptable substitutes.
- Automatic Detector Maintenance Alert: The fire alarm control panel shall automatically interrogate each intelligent detector and shall analyze the detector responses over a period of time. If any intelligent detector in the system responds with a reading that is above or below normal limits, then the system will enter the trouble mode, and the particular detector will be annunciated on the system display, and printed on the optional printer. This feature shall in no way inhibit the receipt of alarm conditions in the system, nor shall it require any special hardware, special tools or computer expertise to perform.
- Pre-Alarm Function: The system shall provide pre-alarm levels of warning to give advance notice of a possible fire situation. Both pre-alarm levels shall be fully fielded adjustable. The first level shall give an audible indication at the panel. The second level shall give an audible indication and may also activate control relays. The system shall also have the ability to activate local detector sounder bases at the pre-alarm level, to assist in avoiding nuisance alarms.
- Software Zones: The FACP shall provide minimum 70 software zones, minimum 5 additional special function zones, minimum 5 releasing zones, and minimum 10 logic zones.
- The fire alarm control panel shall include a walk test feature. It shall include the ability to test initiating device circuits and notification appliance circuits from the field without returning to the panel to reset the system. Operation shall be as follows:
 - Alarming an initiating device shall activate programmed outputs, which are selected to participate in walk test, for 3 seconds.
 - Introducing a trouble into the initiating device shall activate the programmed outputs for 8 seconds.
 - All devices tested in walk test shall be recorded in the history buffer.

SUPERVISORY OPERATION

- An alarm from a supervisory device shall cause the appropriate indication on the system display, light a common supervisory LED, but will not cause the system to enter the trouble mode.

SIGNAL SILENCE OPERATION

- The FACP shall have the ability to program each output circuit (notification, relay, speaker etc) to deactivate upon depression of the signal silence switch.

NON-ALARM INPUT OPERATION

- Any addressable initiating device in the system may be used as a non-alarm input to monitor normally open contact type devices. Non-alarm functions are a lower priority than fire alarm initiating devices.

4.9. CODES AND STANDARDS:

- National Building Code of India – 2016
- Bureau of Indian Standards (BIS) Codes: IS 2189 (2008)
- NFPA-72 (2013)
- Listing and/or Approvals:
 - UL (Underwriters Laboratories Inc.)
 - FM (Factory Manual)

4.10. INSTALLATION

- All fire detection and alarm system devices, control panels and remote annunciators shall be flush mounted when located in finished areas and may be surface mounted when located in unfinished areas.

4.11. TEST

- The service of a competent, factory-trained engineer or technician authorized by the manufacturer of the fire alarm equipment shall be provided to technically supervise and participate during all of the adjustments and tests for the system. All testing shall be in accordance with NFPA 72
 - Before energizing the cables and wires, check for correct connections and test for short circuits, ground faults, continuity, and insulation.
 - Open initiating device circuits and verify that the trouble signal actuates.
 - Open and short signalling line circuits and verify that the trouble signal actuates.
 - Open and short notification appliance circuits and verify that trouble signal actuates.
 - Ground all circuits and verify response of trouble signals.
 - Check presence and audibility of tone at all alarm notification devices.
 - Check installation, supervision, and operation of all intelligent smoke detectors using the walk test.
 - Each of the alarm conditions that the system is required to detect should be introduced on the system. Verify the proper receipt and the proper processing of the signal at the FACP and the correct activation of the control points.
 - When the system is equipped with optional features, the manufacturer's manual shall be consulted to determine the proper testing procedures. This is intended to address such items as verifying controls performed by individually addressed or grouped devices, sensitivity monitoring, verification functionality and similar.

4.12. FINAL INSPECTION

- At the final inspection, a factory-trained representative of the manufacturer of the major equipment shall demonstrate that the system functions properly in every respect.

4.13. 3-CORE 1.5 SQ MM (15AWG) FRLS FLEXIBLE CABLE OR ARMOURED CABLE**Conductor:**

Nos. of cores x size in sq. mm:	3 X 1.5
Material:	Plain annealed copper(Cu)
Type of pair:	Shielded twisted pair
Copper as per Class 1 of IS:	8130/84
Max. d.c. resistance of conductor at 20° C:	12.10 (ohm/km)
Shape of the conductor:	Solid Circular
Outer Sheath color:	RED

Insulation:

Material:	XLPE as per IS 7098(Pt-1)/88, Latest
Nominal thickness (mm):	0.7
Minimum thickness (mm):	0.53
Core Identification:	Red, Black

Armouring:

Material:	Galvanised Steel
Type of armouring:	Round Wire
Nominal size of armour (mm):	1.40

Electrical Parameters:

Approx. overall diameter of the cable (mm):	10
Minimum bending radius:	12 times Overall diameter

MANUFACTURER'S AUTHORIZATION (MAF)

MAF Letter Format (On OEM Letter head with seal)

Date: _____

To,

<<< NAME OF CLIENT/ORGANIZATION>>

Subject: Manufacturer's Authorization Certificate

Tender Ref.: << PLEASE SPECIFY SPECIFIC TENDER REF.NO.>>

Dear Sirs,

This is with reference to the above mentioned Tender.

We hereby authorize <<NAME AND ADDRESS OF INTEGRATOR>> to offer our range of product in their tender bids. Being authorized <<NAME AND ADDRESS OF INTEGRATOR>> may make techno-commercial and commercial proposal for this tender.

Upon being awarded the work <<NAME AND ADDRESS OF INTEGRATOR>> are authorized to install and commission our range of products falling under <<SECTION/PRODUCT CATEGORY>> of this tender.

We as Original Electronic Manufacturers will provide all the techno-commercial and service support necessary to <<NAME AND ADDRESS OF INTEGRATOR>> for this project during the commissioning phase of the equipments and until hand-over.

We also confirm that the items would be serviceable during the warranty period of 12 months and for at least five years thereafter.

Thanking and assuring best of our services at all times.

Yours faithfully

(Seal & Signature)

**LIST OF APPROVED MAKE / MANUFACTURER FOR LOW VOLTAGE (LV) SYSTEMS
MATERIALS (IN ALPHABETICAL ORDER)**

S/No.	Item Description	Specified Brand/Make/Manufacturer
1	2 & 3 X 1.0 Sq. Mm. FRLS flexible cable for Fire Detection & Alarm System	FINOLEX, HAVELL'S, POLYCAB ,R.R. KABLE
2	2 & 3 X 1.5 Sq. Mm. FRLS flexible cable for Fire Detection & Alarm System	FINOLEX, HAVELL'S, POLYCAB ,R.R. KABLE
3	F/UTP CAT6ACabling System – Cable and components	COMMSCOPE-SYSTIMAX, COMMSCOPE-NETCONNECT, PANDUIT-PANNET,SCHNEIDER-ACTASSI
4	Fiber Optics Components (Data & Voice/Telecom, Single Mode) – Cables, LIUs, Shelves, Pigtails, Patch-cords, Connectors, Couplers, Splices	COMMSCOPE-SYSTIMAX, COMMSCOPE-NETCONNECT, PANDUIT-PANNET,SCHNEIDER-ACTASSI
5	Outdoor pole mounted enclosure and wall mounted enclosures for faculty Housing	3M, COMMSCOPE, PANDUIT, RAYCHEM, SCHNEIDER, TYCO
6	IP66 rated 96 core External Splicing Kit for outdoor fiber optics cable	3M, RAYCHEM, TYCO
7	Networking Racks, Data Centre racks, Distribution Racks – from sizes 15U to 42U	APW-VERO PRESIDENT, PANDUIT-PANNET, RITTAL
8	Networking Switches& NMS – Edge/Access, Distribution, Core Switches and all their accessories and options such as fiber optics interface modules and transceivers& NMS.SM and MM fiber optics transceivers shall be original (OEM supplied). All these components shall be from a single OEM.	CISCO, EXTREME NETWORKS, HP
9	Wi-Fi System - Wireless Access Points, Wireless Controller, Wireless licenses etc. All these components shall be from a single OEM.	CISCO, EXTREME NETWORKS, HP-ARUBA, RUCKUS
10	CCTV / Video-Surveillance All types of Cameras (Indoor and Outdoor) – Fixed Dome, Fixed CS-Mount/Box, PTZ	AXIS – (Europe Made), BOSCH – (Europe make), SONY
11	VMS Software Platform	GENETEC, MILESTONE, QOGNIFY (NICE)
12	Servers for VMS Server & Recorder Function	DELL, HP, LENOVO
13	Storage System for CCTV	EMC2, HP, IBM, NETAPP
14	Industrial Ethernet Switch incl. Power supplies	Industrial Ethernet PoE+ Switch incl. Power supplies
15	Client PCs - Hardware/Computers/Workstations	DELL, HP, LENOVO
16	Fire Detection & Alarm System	NOTIFIER, SIEMENS-FIRE FINDER, TYCO-SIMPLEX
17	A3 Size Colour Laser Printer	CANON, EPSON, HP
18	55" HD/DVi Professional Display for CCTV Monitoring	HITACHI, PANASONIC, SAMSUNG
19	Access Control System Readers, Controllers	BOSCH, IDENTIV, LENEL, MATRIX
20	Access Control & Time Attendance Software Application	BOSCH, IDCUBE, MATRIX
21	Electro-Magnetic Locks	ALGATEC, ASSA-ABLOY, BEL

ELV SYSTEMS WORKS MATERIAL SPECIFICATIONS FOR NALANDA UNIVERSITY, RAJGIR

Note: Before approval of the make for supplying the material technical particulars confirming to the TS must be submitted by the contractor.