TECHNICAL SPECIFICATION

1 Scope of Work

The bidder shall Supply, Installation, Testing &Commissioning of Access Control system, IP CCTV System including cameras, Network video recorder system, Management servers, applications / software, access control system equipment, switches and any other items / accessories required for a fully functional system.

The number of cameras and their placement shall be decided in such a way that most critical areas can be monitored. Proximity card reader devices shall be placed as per site requirement. Multi- criteria detectors shall be placed in such a way all the areas to be covered.

2 Functional Requirements

2.1 Access Control System

Control and monitoring for security applies to all entry/exit doors and related areas. Access to buildings, gates, doors is restricted for unauthorized users. Card access system can offer facility managers the flexibility to control these access points.
Smart card reader shall be installed at entry to various rooms as per site requirement in 5th& 6th floor. Each door shall have a door locking mechanism, and a door status indicator. All exit gates shall be open able through push button switches.

In case of fire, the FAS, using addressable outputs shall directly release the door locks controlled by the Access control system.

2.1.1 The system shall provide a mean to control access through nominated doors having electric locking door status monitoring and access control readers. Access rights associated with a presented access card shall be checked for validity based on card or identifier, access area, access time and any other access management function defined in this specification; as stored in access controllers. Access shall be granted or denied, dependant on the access privilege. Access rights shall be programmed in a variety of ways to allow flexibility as defined elsewhere in this specification.

2.1.2 All system communications must be totally integrated with either existing or new LAN networks. Bidder must make themselves familiar with the specific requirements for this project.

2.1.3 Connection to Access Controllers shall be achieved using cabling supporting Ethernet and TCP/IP protocols.

2.1.4 All data communication internal to the system between Access Controller and the Server shall be on TCP/IP Network and should be encrypted and an industry-standard encryption algorithm to a minimum of 128 bit AES.

2.1.5 The system shall report all events to the operator(s) as configured and shall produce and maintain a log of all system events and alarms.

2.1.6 The system shall provide a means for an operator to extract information relative to the event log and system configuration and produce this information in the form of printed reports, screen displays etc.

2.1.7 Comprehensive backup and archiving facilities shall be incorporated as an integral part of the system software.

2.1.8 Access Controllers must support peer to peer communications for input and output communications between Access Controllers.

2.1.9 The Access Controller shall be of **UL listed.**

2.2 IP CCTV System

IP CCTV system shall enable centralized online surveillance of various selected areas and to generate a record for post event analysis. The camera shall be a high resolution, visible at low light capability. The recording shall be in real time motion i.e. 25 frames per second at D1 resolution for each camera. Recording videos shall be kept for 90 days with RAID5 configuration. The camera shall be ONVIF S and G compliant.

One Network Video recorder with required client license shall be used to record & playback the camera videos. All the live view or recorded videos of cameras shall be displayed through client software on proposed workstation.

As an application, the video surveillance will do the following:

- Providing real-time monitoring of a facility's environment, people and assets.
- Recording in case there is a motion in the room
- Recording events for subsequent investigation, proof of compliance / audit purposes
- Shall facilitate motion search on recorded video

~~**2.3** Fire Alarm System~~

~~The proposed Fire Alarm System will be one loop intelligent addressable panel. The loop will consists of detectors & devices making it a total capacity of detectors / devices per panel. The fire alarm panel has a large display. The proposed panel shall be UL listed/FM approved. We have proposed intelligent Multi-criteria detectors on ceiling, on false ceiling wherever applicable & below false flooring. Addressable relay module & monitor modules are proposed in the system for monitoring as well as control requirement respectively. The fire alarm system shall use monitor modules / relay modules / control modules which will operate based on cross-zoning of detectors.~~

CODES AND STANDARDS

The entire installation shall be installed to comply with one or more of the following codes or Standards:

- NBC of India, 2016 amended up to date
- IS 2189.
- British Standards, BS 5839 Part 1 or BS 6266
- NFPA 72 Standards, US

Technical Specifications

1.1.1 Access Controller

The above Access control software shall be capable of monitoring; control of the system shall be powerful enough to enable security managers to manage their site's overall security. The Access Control System (ACS) shall be capable of integrating multiple building functions including access control, alarm management.

The system shall incorporate the necessary hardware, software, and firmware to collect, transmit, and process alarm, tamper and trouble conditions, access requests, and advisories in accordance with the security procedures of the facility. The system shall control the flow of authorized personnel traffic through the secured areas of the facility. The user interface at the host computer (server) shall be a mouse driven graphical user interface (GUI) allowing the user to open and work on multiple windows simultaneously.

a) The Controllers shall be UL certified and conform to UL standards.

b) Flash memory for easy online software updates.

c) Supports two-man rule and escorted access for increased security

d) Configurable audio tones to indicate valid card read, invalid card read, and other types of events.

e) Large alarm buffer protects integrity of alarm data

f) Dynamic memory management allows maximum storage of card holders and transactions

1.1.2 Proximity card readers ~~Biometric Fingerprint Card Reader & Enrolment Biometric Reader~~

Reading element	: Optic sensor
Timing	: Card read < 0.5 sec
Output	: Same card data as in the Input in case of validation. No data in case of no validation Access decisions shall be made at each controller.

Access criteria changes shall be downloaded from the controller automatically, according to a pre-programmed schedule.

All card readers shall unlock the controlled door within 0.2 seconds of the completion of the access attempt. The completion of the access attempt is defined as the end of the card shown for card only entry. This time delay shall never be exceeded, regardless of system loading.

The following fields shall be transmitted:

- Time or entry or exit
- Point of entry or exit
- Access granted or denied
- Card number
- Cardholder's name

Each card reader shall be capable of automatically switching the current access criteria at a door at different times of the day, based on access control data received from the site controller.

The following access criteria modes are required:

Free access - door is unlocked, no card entry is required

Secure access - door is locked (secure). A successful card attempt is required for valid entry. Door rescues after access attempt.

Pending access - door is locked (secure). Door switches automatically to unlock (free) upon first successful access attempt during pending mode period, or vice versa (see next clause). Within pending mode, two options shall exist:

The card reader is operating in secure access mode. When the first valid entry occurs, the card reader shall automatically set the access criteria for this reader to free (public) access.

The card reader is operating in free (public) access mode. When the first valid "access attempt" occurs, the card reader shall automatically set the access criteria for this reader to secure (card-required) access.

1.1.2.1 Database management:

The system shall create and maintain a master database of all cardholder

records The System shall support various databases – Microsoft SQL, MySQL and Oracle.

Alarm Input Point Reporting Delay: The ACS shall allow the operator to apply an input point reporting delay period from 0-60 seconds for each input point terminal. The default setting for each input point reporting delay shall be 0 seconds.

Alarm Input Point Suppression: The ACS shall provide an alarm input point suppression facility such that the operator may define a time zone suppression period for each individual input point. Alarm conditions for suppressed input points shall not be recorded or archived by the system, however, trouble conditions will be recorded.

Alarm graphics (maps): The alarm-graphics portion of the system shall provide dynamic colour alarm graphic maps with the following functions: User definable graphic maps to depict input and output point conditions, reader status, and sub-map attachments in the ACS.

The ACS shall support the importing of most bitmap file format graphics produced with any graphic drawing program such as TIF, BMP or JPG file format. Vector file formats are not acceptable.

The ACS map program shall support the importing of most bitmap file format graphics to produce custom icons for all map attachments (input, output, reader, etc.).The ACS software shall be capable of storing a number of graphic maps.

The ACS shall provide a palette that includes six categories of pre-defined alarm map icons:

Input: representing a user-defined alarm input point located anywhere in the system. The input point icon shall flash, change colour, and the computer's internal sounder shall beep when an alarm condition exits. It shall be possible to click on the icon to respond to the alarm condition or move directly to the alarm queue window to respond to the alarm. Each alarm- input icon shall have a pop-up box that indicates the point's current state (open, short, alarm/active, secure).

Output: representing a user defined output point located anywhere in the ACS. It shall be possible to click on the icon to set or reset the output point. In addition, it can display the set or reset status of point.

~~**Map layer:** representing that lower level maps associated with the top layer map exist in the system. It shall be possible to navigate through the map layers by clicking on the map layer (up and down) icons.~~

Reader Terminals: reader icons shall have the capability of displaying: held open, forced open, locked, unlocked, unknown, override, up and down. Panels: representing a system panel controlled by the ACS. Panel icons shall have the capability of displaying the up or down status of the panel.

I/O Terminals: I/O terminal icons shall have the capability of displaying the up or down status.

Alarm handling: The alarm handling portion of the system, which consists of the point contacts, and the Alarm monitoring Window shall provide the following functions:

The Alarm Monitoring Window shall be capable of being sorted by any column. It shall also have displayed the total number of alarms in the queue and the number that are pending. The Alarm Monitoring Window shall have the capability to bring up the map to the input, which is highlighted in the window.

User definable alarm message/instructions description: The system shall provide the ability to assign alarm message/instructions to each state of an input point ('Open', 'Short', 'Alarm/Active', and 'Secure.')

Alarm message "pick list": all alarm message names and associated descriptions shall appear in the form of a pick list from which the operator may select an appropriate alarm name and message from all alarm messages defined in the database by the operator.

1.1.2.2 Event processing:

Panel card events: the ACS shall provide the capability for the user to define a panel card event, which may be executed by a cardholder at a reader equipped with a keypad. For each 'card event' the following data may be defined by the User:

- Alphanumeric event name
- Access code to control the triggering of the event (card activated event)
- ~~Event triggers type (card only, card + PIN, card + PIN + code, card + code, void card)~~
- Event Privilege level (0-7)
- Duration of the event execution (0-1440 minutes)
- Input point group to be suppressed or not
- Output point group to be activated or not
- Door strike operation enabled/disable
- Reset panel alarm relay

Host events:

Triggers: the ACS shall provide the operator with a scrolling list of the following event sequence triggers as a minimum that may be combined with the event sequence logical operators listed below to program a custom sequence of events. The ACS shall be delivered with this entire list functional whether or not these features are implemented by the User upon initial installation.

Actions: the ACS shall be provide a scrolling list of the following event sequence actions as a minimum, and allow the user to attach one or more actions to one or more of the event sequence triggers listed above to program a custom sequence of events.

- Enable anti-passback
- Disable anti-passback
- Unlock door control relay
- Lock door control relay
- ~~Enable timed override of door control relay~~
- ~~Set time zone for PIN code suppression~~
- ~~Set time zone for reader~~
- ~~Set time zone for reader override~~
- ~~Enable reader override~~
- ~~Disable reader override~~
- ~~Enable soft In-X-It~~
- ~~Disable soft In-X-It~~
- ~~Enable local timed override~~
- ~~Disable local timed override~~
- Lock all doors
- Unlock all doors
- Enable history upload
- Disable history upload
- Include time zone in access decision

- Ignore time zone in access decision
- Set controller relay
- Reset controller relay
- Enable input point group
- Disable input point group
- Set output point group
- Reset output point group
- Display a user defined message in a pop-up window
- Print user defined message on any printer
- System Database backup
- System Panel Download
- Display map
- Event Counters

Time zones: The ACS shall provide the capability for the user to define time zones with the following identification and configuration parameters.

1.1.2.3 Alphanumeric name

Alphanumeric description Allowance for up to eight periods, four active and four inactive, during each day of the week and each of three different holiday types. Any day of the year may be designated as a holiday; each defined as one of three holiday types.

1.1.2.4 Other Features:

User defined cardholder database fields: The system shall support up to an unlimited number of user defined data fields, which may be used to store information for each cardholder. Each field may be of a type: alphanumeric text, numeric, date, toggle (Yes/No). The ACS shall provide standard menu items, which shall allow the operator to define these cardholder database fields at anytime. The system shall remain on-line while user defined cardholder database fields are added or edited

~~The System shall support the capturing of high quality finger prints and encoding the finger print into the card during enrolment process that is native of System.~~

~~Also the System shall allow operators to capture and store the fingerprint to the System database. The fingerprints shall be captured using a biometric reader and an enrolment reader shall be used for fingerprint encoding.~~

Event and Transaction History: The ACS shall maintain a record of all alarm, card transaction, and system exceptions, which take place, and provide a means for a user to access this information. It shall be possible to print information in the log in real-time or by a report.

Anti-Passback Control: The ACS shall provide the capability to prevent more than one person from gaining access to a controlled area by recognizing when a cardholder who is granted access is passing back the card to another person to use the same card to gain access. If so programmed, an alarm may be generated if the anti-passback rules are violated by the cardholder. It shall be possible to define on a reader by reader basis, which readers are subject to anti-passback rules.

Cardholder Definition: The ACS shall provide the capability for the user to define Cardholders with the following identification and operating parameters.

- Cardholder name (first, middle, last)
- Cardholder address
- Cardholder phone number and extension number
- Validation period using start and void dates
- Department and Company fields from selection list of user defined departments and companies
- Unlimited number of user defined cardholder fields. The ACS shall provide the capability to use these fields in filtering reports.

Badge Definition: The ACS shall provide the capability for the user to define Cardholders with the following Badge identification and operating parameters on a per badge basis.

- Badge number assignment
- Issue level (0-7), only (1) per badge
- Validation period using start and void date and time
- Globally disable badges in all partitions
- Executive privilege enabled or disabled
- Active/Disable badge toggle button
- Trace enabled or disabled
- Override enabled or disabled
- PIN code (4 or 5 digits)
- Badge event privilege level
- Assign eight Access Groups and Time zones per Badge

System Status Display: The ACS shall provide a dynamic system status summary display that graphically indicates the following status information, filtered by panel or terminal. All status display information shall be summarized in a single window.

Alarm routing: The ACS shall provide the ability for the user to define which input points or groups of input points are displayed on each ACS Operator Workstation Terminal (OWT) computer. The system shall provide a report showing which input points are routed to each OWT.

Control points: The ACS shall provide the ability to define input points as control points to be used in input/output linking and event processing sequences of operation. Control points shall not enter the alarm queue and shall not require that an operator acknowledge them when they change state. The control point activity will however, be automatically logged to the history file.

Real Time Printer: The ACS shall be capable of printing to a network accessible printer as well as printing from an LPT port. The ACS shall be capable of printing with the following parameters:

Be able to specify printing of the following items, independent from each other:

- Input Point Alarms
- System Exception and Event Messages

- Access Trace
- Access Deny
- Access Grant
- Entry/Exit Central
- Audit Trail.

IP CCTV System

1.2.1 System Description

The system shall include all network video cameras, network switch, server hardware, video management software, cabling, supports, hardware, software and interfaces to provide complete system. The system shall seamlessly integrate with the access control system and security management control system. The system shall be expandable to encompass the entire site.

A network camera combines a camera and computer in one unit, which includes the digitization and compression of the video, as well as a network connector. The video is transported over an IP-based network, via network switches. This represents a true network video system, and is also a fully digital system, where no analogue components are used.

A network video system using network cameras adds the following advantages:

- High resolution cameras (megapixel)
- Consistent image quality
- Power over Ethernet
- Full flexibility and scalability

The CCTV system shall comprise minimum of the following equipments (components) along with CAT6 cables, cable containment and associated accessories, hardware to provide a complete and operational CCTV system for alarm assessment and general surveillance purposes. Provide following minimum operational features:

- Network camera,
- Network switch with patch panel and necessary converters (if required)

1.2.2 Viewing Station

1.2.3 Indoor High Definition Resolution IP Network Dome Camera

	Video:	
i.	Video standards	Dual H.264 and MJPEG stream
ii.	Sensor	1/2.7" 2MP progressive CMOS/CCD image sensor
iii	**Resolutions and frame rates:**	**PAL**
iv	Resolution	1920 x 1080
	Video out	
v	Signal	ONVIF S and G
vi	Connector	RJ-45 10BaseT / 100BaseTX
vii	Video S/N	> 50 dB
viii	**Sensitivity:**	

	Day/Night	Yes
	Color	0.01 lux
ix	Wide Dynamic Range	120DB
x	White balance	Yes
	Electronic shutter	
xi	PAL	1/5 – 1/10000 s
	Optical	
xii	Lens	Varifocal 2.8mm (W) – 12 mm (T)
xiii	Iris control	Automatic
	Camera Tampering	
xiv	Camera Sabotage	Alarm should be generated
	Software Control	
xv	Unit configuration	Via web browser or Configuration Manager
xvi	Motion detection	Yes
	Alarm	Yes; 1x Alarm In & 1x Alarm Out
	Network	
xvii	Protocols (Any of the following)	TCP/IP, UDP, HTTP, HTTPs, SMTP, SNMP, DNS, DHCP, NTP, FTP, RTSP (RTP), IGMP v3, UpnP, CIFS, NFS, IEC802.1x, ONVIF
xviii	Ethernet	10/100 Base-T, auto-sensing, half/full duplex, RJ45
xix	POE	IEEE 802.3af compliant
xx	Operating Temperature	0°C to 50°C
xxi	Operating Humidity	0% to 80% (Non Condensing)
	CERTIFICATES & APPROVAL	
xxii	Safety	UL
xxiii	Ingress protection and Vandal	IP66, IK10

1.2.3. Network Recorder

The Network video Recorder shall be capable to seamlessly integrate to the video analytic software, if and when added to the system.

Sl No	Specification	Minimum requirement
1	Type	Rack-mountable, Dedicated Network Video Recorder with suitable hardware to connect up to 32 IP cameras (i), offered storage is not an externally attached device to NVR, the total recording storage requirement shall be met through internally installed HDD itself. The bidder to submit the storage analysis for required no of cameras for a period of **90 days** @15fps on minimum D1resolution. All channels must support recording resolution of D1@15fps. (ii) Additional hardware/ software/ license, if any required by the bidder to meet its offered solution, should be considered accordingly by the bidder in its offer.
2	Storage capacity	Each NVR storage unit should be provided with usable 8 SATA HDD slots with provision of future expansion of HDD Slots using eSATA
3	Operating system	Linux or Embedded or Microsoft
4	Video compression	H.265/ H.264, MJPEG/MPEG
5	Recording support	The offered NVR must be able to support simultaneous recording of 32 IP cameras at D1 resolution at 15 fps
6	Network Protocol Support	HTTP/HTTPS, TCP/IP, RTSP, UDP, NTP, DHCP, IPC Search
7	On-board diagnostics	Web based support for system configuration & Diagnostics
8	Documentation	Installation guide, Operation & Maintenance Manuals, Installation CD/DVD for licensed software
9	Input Voltage	100~240 V AC, 50/60 Hz.
10	Compatibility	The supplied NVR must be compatible in all respects to the cameras being supplied at the locations
11	Operating temperature	10°C ~ 40°C or better
12	Operating Humidity	20% to 80% RH, non-condensing
13	HDD	HDD Hot swap, 8 bays SATA HDD, up to 8TB storage.
14	Product Safety	To comply with CE, FCC, UL
15	Details Required with offer	Bidder to submit the details of complete offered solution (Item make, model/part code, block diagram etc.) as stated above along with the offer.

1.2.5. 27U" FLOOR MOUNT RACK

The Network shall be accommodate to storage server, core switch, network switch, light interface modules, patch panel etc. Shall also be a provision to add more switch and server. Network Rack shall Compliance the following specification

SL No	Specification	Minimum requirement
1	Size	Min 27U
2	Type	Network
3	Mount	Floor
4	Caster Wheel	4 No's with Lockable
5	Mounting Size	19"
6	Cable Manager	As Required
7	Shelves	Min 4
8	Doors	Front and Rear Lockable Glass Door
9	Power Strip	Min 10 No's of 5/15A
10	Cooling Fan	4 No's on Top

1.3 Cables & Conduits

Cat 6 cables shall be used for connection to the switch from the camera/ access controller

The 2 Core 1.5 Sq mm cable connecting the Detectors/ Field devices to Fire alarm Panel shall be PVC insulated copper, multi strand, FRLS cables shall be 1100V grades.

Cables connected to devices shall be given 'S' loop on both the sides of the devices which shall be properly clamped to the ceiling. Loop shall also be left where cables connect sounders, panels, dampers, etc. Appropriate glands shall be provided where the cable enters the junction box.

All the cables and wires shall be tagged for proper identification. Wires shall be identified by ferrules at junction and cables by colour bands.

Cat 6 Cable

i.	Conductors	23 AWG solid bare copper or better