غرفة تجارة وصناعة الشارقة
Sharjah Chamber of Commerce & Industry

REQUEST FOR TECHNICAL PROPOSALS

Supply and Installation of CCTV System

SHARJAH CHAMBER OF COMMERCE & INDUSTRY

APPROVED

Bid issue date:

Deadline for submission of proposals:

TABLE OF CONTENTS

Section A - Instruction to Bidders

1 - SITE SURVEY 4

2 - PACKING AND LABELLING OF PROPOSALS 4

3 - SUBMISSION OF PROPOSALS 4

4 - PROPOSAL CONTENTS 5

5 - RFP TERMS AND CONDITIONS... 6

6 - INCOMPLETE AND LATE OFFERS: 6

7 - INQUIRIES.. 6

8 - ALTERATION OF PROPOSALS 6

9 - BIDDER RESPONSIBILITY 6

10 - ELIGIBLE BIDDER.. 6

11 - CLARIFICATION 7

12 - EVALUATION OF PROPOSALS...7

13 - AMENDMENTS 7

14- CONFIDENTIALITY...7

15 - OWNERSHIP OF PROPOSALS...7

16 - BID CANCELLATION..7

17 - DISCUSSION/NEGOTIATION 7

Section B – Terms of References

1 - About Sharjah Chamber of Commerce and Industry (SCCI).. 8
2 -PURPOSE AND OBJECTIVES OF THE RFP 8
3-Drawing References.. 8

4- SCOPE OF WORKS.. 8

1.1. CCTV Cameras,
1.2. CCTV Analytics
1.3. CCTV Storage for 90 days
1.4. Video Management System/ Video wall for the control room
1.5. PC Work Stations and Display Monitor.

5. CCTV SPECIFICATIONS.. 9

5.1 Indoor Cameras...9

5.2 Outdoor Cameras.. 10

6. NETWORK STORAGE (NVR).. 11

7. VMS SOFTWARE MAIN FUNCTIONALITES... 11

8. VMS SERVERS... 13

8.1 VMS SERVER TASKS 13

8.2 Preferred Camera server Tasks 13

8.3 Availability Functionality after Failover 15

8.4 Failover and Failback Mechanism 15

1. VIDEO ANALYTICS SERVERS ….. 15

2. HARDWARE.. 17

3. SYSTEM SOFTWARE... 21

4. APPLICATION SOFTWARE FUNCTIONS.. 21

5. SERVICES... 59

9. COMMUNICATION NETWORK.. 60

10. INTERFACES.. 60

11. CAMERA LOCATION... 60

12. RULES AND REGULATIONS... 60

12.1 SIRA REGULATIONS.. 60

12.2 SHARJAH POLICE REGULATIONS 60

13. ACCESS CONTROL SYSTEM 61

14. BOQ 62

Section A

Instruction to Bidders

Bidder is requested to read the documents carefully to be able to submit aresponsive proposal. In submitting the proposal, contractor must respect all instructions,forms, Terms of Reference, contract provisions and specifications contained in thisdocument. Failure to submit a proposal containing all the required informationanddocumentationwithin the deadline specified will lead to the rejection of theproposal.

1 -SITE SURVEY

All suppliers are requested to visit SCCI head office building for a walk through inspection to investigate the hardware available in SCCI prior submitting their proposal. Submitting proposals without the Site survey would be at the supplier's own risk.

Date of Site Survey:
Time of Site Survey:
Contact Person:
Telephone No:
Important Note: Above contact is only for the purpose of the Site Survey. Please note that the Site Survey is only for the suppliers to check the project delivery site. Suppliers are strictly not allowed to inquire about any financial or procedural questions. Any deviation to such rules will eliminate the supplier from participation in this tender.

2 - Packing and Labelling of Proposals

Each submitted proposal must comprise a Technical offer and a Financial offer, each ofwhich must be submitted separately in sealed envelopes. Each Technicaloffer and financial offer must contain one original, clearly marked "Original", and 1copy, marked "Copy".

3 -Submission of Proposals

Proposals must be submitted hand delivery directly to the SCCI in return for a signed and dated receipt to the following address:

Noura Jasim Almaazmi,
Head of Procurement department,
Sharjah Chamber of Commerce and Industry,
Post Box No. 580, Sharjah, UAE.

Note: Proposals submitted by any other means (fax or e-mail) will be rejected.Any deviation from these instructions (e.g., unsealed envelopes or references to price in the technical offer) is to be considered a breach of the rules, and will lead to rejection of the proposal. The pages of the Technical and Financial offers must be numbered.

4 - Proposal Contents

4.1 Technical offer

The Technical offer must include the following documents:

1. Table of contents, including page numbers.
2. Full contact details of the key person in the company in case of anyclarification requirements.
3. Letter of Submission on the contractor's letterhead signed andstamped by the person in charge or company's authorized representative acknowledging the supplier's agreement of the terms and conditions of this RFP and certifying that all information offered in the submitted proposal are true, accurate, and complete.
4. An executive technical summary including Items, Technical Specifications (Bill Of Quantities) unpriced, demonstrating the supplier understands of the RFP's requirement, including the specification of requested item, delivery andinstallationschedule.
5. Copy of valid trade license / legal registration, Documents/agency registration in the UAE
6. Business references from different clients that shows that the Supplier has a satisfactory performance record. Supplier is required to include details of points of contact (name, address, telephone number, etc.) for such references. The Supplier should have implemented minimum five CCTV projects and the suppliers have to list such projects. Supplier must submit in his quotation the company references for similar CCTV project or scope of work.
7. Soft copy of the technical proposal ONLY "with no reference to commercial offer".
8. The Supplier must be authorized dealer of CCTV system.
9. The supplier must have approval from civil defense or police authority.

Important Notes: After the bid opening of the TECHNICAL proposals and incase any bidder did not submit the required documents state above, the proposal will be administratively rejected without further consideration for review.

REVEALING THE FINANCIAL OFFER IN TECHNICAL OFFER WILL LEAD TO THE REJECTION OF THE PROPOSAL.

4.2 Financial offer

The Financial offer must be presented as an amount in U.A.E currency (DHS), inclusive of all applicable tariffs and /or taxes and must be submitted using the attached template in filling the prices (Annex III). Bidder has to put the prices showing the unit price per item intended to be proposed.

- Payments under this contract will be made in U.A.E currency (DHS).
- The hard copy of the priced list should be submitted stamped and signed.
- Soft Copy (CD) of financial offer

5- RFP Terms and Conditions

- Failure to accept the terms and conditions of this RFP at time of submission of proposal may result in giving the award to the next supplier.

6 - Incomplete and Late Offers:

- Incomplete and late proposals will not be accepted. It is the bidder responsibility to ensure that the proposal is submitted complete, on time and in accordance with the RFP terms and conditions. Late proposals shall be returned back.

7 - Inquiries

- Suppliers may submit questions in writing through e-mail to the following address before the deadline stated in the above timetable,

Contact Name:		KHALIFA ABDUL REHMAN BIN HADDAH
E Mail	:	Khalifa@sharjah.gov.ae
Phone No	:	06-5938595

- Any clarification to be issued by the Services Sector will be communicated in writing to the supplier before the deadline stated in the timetable above. No further clarifications will be given after this date.

8 - Alteration of Proposals

Suppliers may alter their proposals by written notification prior to the deadline for submission of proposals stated in this RFP. No proposals may be altered after this deadline.

9 - Bidder Responsibility

It is the responsibility of each supplier before submitting a proposal:

a) To consider federal and local laws and regulations that may affect costs, progress, performance or furnishing of the service.

b) To study and carefully correlate supplier’s knowledge and observations with the contract documents and such other related data.

c) To promptly notify the section Head of Procurement & Services Sector of all conflicts, errors, ambiguities, or discrepancies which supplier has discovered in orbetween the contract documents and such other related documents.

10 - Eligible Bidder

Bidders considered eligible to submit proposal is defined as the entity /organization that is legally registered to do business in UAE and can provide a valid certificate of legal registration/ trade registration license. The bidder must be authorized partner of CCTV system.

11- Clarification

During the evaluation process, SCCI may request additional information from suppliers if it is necessary for further clarity in regards to the submitted proposal.

12 - Evaluation of proposals

Technical evaluation of bids

- All suppliers have to comply with 80% of the mandatory requirements stated in Vendor Risk Assessment form to be eligible for the completion to the technical evaluation stage.
- The quality of each technical offer will be evaluated in accordance with the evaluation factors specified in this document.
- No other award criteria will be used. The award criteria will be examined in accordance with the requirements indicated in the Terms of Reference.

13 – Amendments

During the proposal submission period, if the SCCI decides to modify/change any requirements of the RFP, the modifications shall be released through the issuance of an amendment to the RFP. Any amendment will be issued in writing and will be sent to all suppliers.

14 - Confidentiality

The entire evaluation procedure is confidential and all proposals are for official use only and may be communicated neither to the bidders nor to any party other than the SCCI.

15 -Ownership of Proposals

The SCCI retains ownership of all proposals received as part of this tender. Consequently, suppliers have no legal right to have their proposals returned to them.

16 -Bid Cancellation

The SCCI has the right at any stage in the tender process to cancel the whole tenders without justification to any of the suppliers. In the event, Suppliers will be notified in writing of the cancellation by the SCCI.

17 - Discussion/Negotiation

Although proposals may be accepted and a contract awarded without discussion, the SCCI may initiate discussions should clarification or negotiation be necessary. Bidders should be prepared to provide qualified personnel to discuss technical and contractual aspects of the proposal.

Section B – Terms of References

1 -About Sharjah Chamber of Commerce and Industry (SCCI)

Sharjah Chamber of Commerce and Industry –(SCCI) was established in order to effectively and vitally participate in the organization of economic life and the prosperity of its trade, industry and professions sectors on all levels and in cooperation with the concerned establishment and bodies and local departments. The chamber is keen to include in its membership all the companies and establishments practicing economic activity in the emirate whether it is trade, industries or professions. It follows the economic and civilization development witnessed by United Arab Emirates a matter that naturally requires change on the different services and the activities of the chamber.

2 -Purpose and Objectives of the RFP

The purpose of the Request for Proposal (RFP) is to present the scope of works for the CCTV system, analytics and Storage system and Arm barriers for the SCCI building according to the international codes and regulation and in accordance with SCCI requirements. The objective of the project is to monitor the total building by CCTV system

3-**Drawing References**

1. **Basement CCTV System**
2. **Ground floor CCTV System**
3. **First Floor CCTV System**
4. **Roof floor CCTV System**

4- Scope of Works

The document describes the scope of the following:

4.1 CCTV Cameras,
4.2 CCTV Analytics
4.3 CCTV Storage for 90 days
4.4 Video Management System/ Video wall for the control room
4.5 PC Work Stations and Display Monitor.

The scope of works described here after are classified as follows:

1. SCCI Indoor CCTV System
2. SCCI Outdoor CCTV System
3. Camera Systems for SCCI building monitoring

General

The scope of work shall include but not limited to supply, design, detailed engineering fabrication, installation of the hardware, software, wiring, cabling, labor, supervision, management control, testing and commissioning, system interfaces of the supplied equipment's, providing system training, operator training, user manual for the total solution including all hardware, software, materials, services and support etc. which are required to provide a turnkey an integrated Video Surveillance System for SSCI building. The scope shall include operation and maintenance within the warranty period of 12 months for all supplied equipment starting from expiry of the Defects Liability Period of one year.

Any software and firmware upgrade/ enhancement/ engineering changes applicable to the hardware and software supplied should be provided for the warranty period within a period of one month from the date of release.

Providing detailed architecture diagram of t Test & development, Quality and Production environment setup for optimum performance, security, scalability and desired uptime requirement. Should include all other supporting material as per the requirement to ensure smooth implementation, in that context, it is a 'turn-key' assignment.

The system integrator will need to provide a detailed implementation plan including the architecture diagram, strategy, approach, and delivery of materials, specific issues, and their resolutions, detailed implementation and post-implementation processes and procedures.

Bidder has to provide the services for the configuring and installing the hardware, deploying and installing the system software as per the requirements (porting of the application)/testing /integration of various hardware and software, as may be needed at SCCI without any additional cost for the period of 1 years from the date of installation for the supported items.

Bidder has to collaborate, coordinate and deploy workforce to ready the entire project setup. Bidder must build in the cost for the same, if any under implementation services.

The CCTV is interfaced with SIRA approved ANPR and provision to integration of ARM Barriers with ANPR must be there for future.

5. CCTV SPECIFICATIONS

5.1 Indoor Cameras

The camera can be mounted at the indoor environments such as offices, receptions, store….

Specification for Indoor cameras

5.1.1 Fixed Dome Camera

- 2 Megapixel Full HD Network IR Dome Camera Max. 2M (1920 x 1080) resolution,
- 2.8 ~ 12mm (4.3x) varifocal lens
- 0.095Lux@F1.4 (Colour), 0Lux@F1.4 (B/W : IR LED on),
- 30fbs@all resolutions (H.264), H.264,
- MJPEG dual codec,
- Multiple Streaming,
- Motion detection,
- Tampering,
- DWDR,
- Micro SD/SDHC memory slot,
- PoE,
- IR viewable length 15m,
- Hall way view support (Rotate 90°/270°)

5.1.2 WDR Dome Camera

- 2 Megapixel Full HD Network Dome Camera Max. 2M (1920 x 1080) resolution,
- Full HD(1080) resolution,
- 60fs@ 1920 x 1080,
- Super light Enhancer,
- 0.1Lux·Enhanced WDR (120dB)/ 30fbs @2MP WDR,
- Built-in 3~ 8.5mm(2.8x) varifocal lens 3MP DC Iris 2.8 ~ 12mm (4.3x) varifocal lens,
- IR Corrected,
- H.254 & MJPEG dual codec Box camera Mount

5.1.3 Box Camera

- 2 Megapixel Full HD Network weatherproof IR Dome Camera Max. 2M (1920 x 1080) resolution,
- 2.8 ~ 12mm (4.3x) varifocal lens
- 30fbs@all resolutions (H.264), H.264,
- MJPEG dual codec,
- Multiple Streaming,
- Motion detection,
- Tampering,
- Micro SD/SDHC memory slot,
- PoE,
- IR viewable length 20m,
- IP 66,
- IK 10

5.1.4 Fish Eye Camera

- Max. 5M (2560 x 2048) resolution
- Various viewing composition, 6 dewarping view mode
- On board dewarping, Digital PTZ / Bi-directional audio
- WDR (60dB), MD, AD
- micro SD/SDHC/SDXC memory slot

5.2 Outdoor Camera

The camera can be mounted at the outdoor environments such as roof area, outside building….

Specs for Outdoor cameras

- 2 Megapixel Full HD 32x Network weatherproof PTZ Dome Camera,
- 4.44 ~ 142.6mm(32X) optical zoom,
- 16x digital zoom,
- PoE+,
- SD/SDHC/SDXC memory slot,
- Bi-directional audio support,
- IP66/NEMA4X/IK10,
- Day & Night (ICR),
- WDR (120dB),
- Intelligent video analytics

6. NETWORK STORAGE (NVR)

The storage of the NVR should be complies with SIRA law for 90 days as minimum, moreover the NVR should be cover all the cameras at the site.

High-density chassis, 4U chassis: Up to 24 HDDs.

Up to 24TB capacity for each HDD

32 channel NVR

Supports RAID 0/1/5/6/10/50/60

Third-party Cameras Support (ONVIF)

Supports camera access through RTSP,ONVIF, and PSIA protocol.

Automatic network replenishment (ANR), timely uploading and video loss alarm.

Supports both CVR and IPSAN.

Search, play and download videos by video type or video time.

7. VMS SOFTWARE MAIN FUNCTIONALITIES

THE SYSTEM SHALL SUPPORT MUTIPLE CAMERA SERVERS, WITH NO SOFTWARE-IMPOSED LIMIT TO THE NUMBER OF CAMERA SERVERS USED IN THE VMS. PREFERRED CAMERA SERVERS

The Preferred Camera Server(s) manage all camera operations during normal operation of the system. They must be capable of supporting a large amount of disk space for online video storage and access to high capacity archiving mechanisms for the transfer of stored video to off-line media.

GENERAL

The Video Management System (VMS) shall be designed and developed to the following standards:

- ISO 9001(2000)
- ISO/IEC 15504 Level 3 or higher (SPICE 2.0 Software Process Improvement and capability Determination)
- SEI CMM Level 5 or higher (American Software Engineering Institute – Capability Maturity Model)

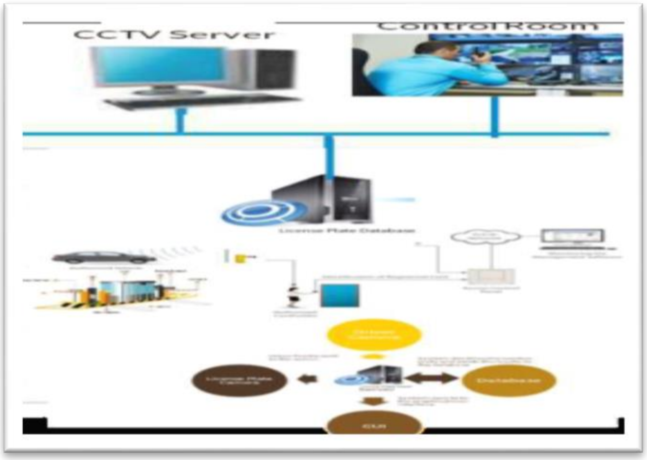
Reference Standards (Cameras): Provide systems that meet or exceed the requirements of the following publications and organizations as applicable to the work of this Section.

- Canadian ICES-003.
- Canadian Standards Association (CSA)
- Conformity for Europe (CE)
- Electronics Industry Association (EIA)
- Federal Communication Commission (FCC)
- Joint Photographic Experts Group (JPEG)
- National Television Systems Committee (NTSC)
- Phase Alternating Line (PAL)
- Underwriters Laboratories Inc. (UL)

The Video Management Systems shall include:

- (Redundant) VMS servers
- (Redundant) Camera Servers
- Mobile Client Video Streaming Servers
- Video Analytics Servers
- Operator Stations
- Network connected cameras and/or network connected video encoders
- Network infrastructure, including network-based storage solutions

The following diagram explains the relationship of these system components:



8. VMS SERVERS

The VMS server shall provide a central fault tolerant repository for all configurations and run time information for the complete system.

8.1. VMS SERVER TASKS

The VMS Server shall:

- Manage the system VMS containing:
- System configuration
- System Redundancy configuration for both VMS and Camera Servers
- Distributed system data for connection to remote Digital Video Management Systems
- Details of IP Camera and /or Encoder functional capabilities
- Camera configuration and settings
- Video Encoder and/or IP Camera Input/output configuration and settings
- Video stream profile configuration for Live and Recorded video
- Details if run time information such as recordings and audit logs
- Configuration of operator views showing multiple camera layouts
- Schedules for recording, Input monitoring, Output switching and video analytics
- Operator security details
- Configuration of Surveillance and Alarm Monitors
- Configuration of IP CCTV Keyboards
- Configuration of Video Analytics including:

  Video Motion Detection

  Intelligent Video Analytics

  Camera Tamper Detection

  Configuration of Video Wall Clients
- Manage communication between the Operator Stations and the Camera Servers

- Support connection to multiple Security System of Control System servers simultaneously
- Each connected server shall be able to receive alarms, activate events and view live of recorded video from the VMS
- Report any camera failures or recording failures to the integrated control system or Security system
- Provide a full audit log of system activity including system status and operator actions

8.2 Preferred Camera Server Tasks

The Camera Serve shall:

- Manage live video and/or video and audio from Video Encoders and IP Cameras
- Transmit live and/or recorded video and audio/video to Operator Stations
- Transmit live video to Surveillance Monitors or Alarm Monitors
- Transmit live video to the Analytics Server(s) for processing using video analytics algorithms
- Receive analytics events from the Analytics Server(s) and perform actions on these events based on pre-configured settings
- Receive camera control commands from Operator Stations or Operator Keyboards and then send the commands to cameras
- Store live video and/or video and audio to hard disk
- Transmit previously recorded video and/or audio/video to Operator Stations
- Archive previously stored video and/or audio/video to media storage location for later archiving
- Retrieve archived video and/or audio/video from storage media
- Analyze live video for events of interest using both simple and Advanced System Format (asf) formats so that the recording can be viewed using standard video players including Microsoft’s Windows Media Player.
- Provide the ability to monitor cameras for tampering including:
- Changed field of view
- Blurred image
- Camera blinded or covered
- Receive input events from the digital input ports of IP cameras or video encoders and react to these events in a pre-configured manner including but not limited to:
- Start recordings on 1 or more cameras
- The VMS ability to replay recorded video shall not be affected by the operational status of the Camera Server that performed the original recording. In the event that the original recording Camera Server is not available, any operational Camera Server shall be able to support the replay of the applicable recorded video if it has logical access to the video data files.

8.3 Available Functionality after Failover

The following functionality continues to be available after a Camera Server failover:

- Live video, including PTZ and camera control
- Processing of Video Analytics
- Processing of Camera Tamper Detection
- Video recordings, including scheduled recordings
- Recording playback, including searching for recordings when video was recorded to a network location
- Archive, restore, delete and export of video clips when video was recorded to a network location
- Triggering of input and output devices, including scheduled triggering
- Video Loss Alarms

The failover of cameras between Preferred and Backup Camera Servers shall be transparent to system operators ad shall not require the operator to reconnect their Operator Station to re-establish access to live or recorded video.

8.4 Failover and Fail Back Mechanism

The failover and fail back mechanism between Preferred and Backup Camera Servers shall be configurable and support both automatic and manual operation.

Automatic failover shall be triggered by the system in the following instances:

- The system detects that the Camera Server does not have an available, healthy storage volume for recordings
- The Camera Server has suffered a deadlock in operation
- The free space for a recorded location has reached a minimum predefined threshold

Manual failover and fail back support shall always be available if required via button on the Operator User Interface, provided the Operator has the correct security level.

It shall be possible to enable or disable the use of automatic failover for each Preferred Camera Server individually. When enabled, it shall also be possible to set the duration of the delay period that the Preferred Camera Server must be in a failed state after which the VMS shall initiate a failover. It shall also be possible to set the level of alarm associated with a Preferred Camera Server failure event.

It shall be possible to enable or disable the use of automatic fail back for each Preferred Camera Server individually. When enabled, it shall also be possible to set the duration of the delay period that the Preferred Camera Server must be in a healthy state after which the VMS shall initiate a fail back. It shall also be possible to set the level of alarm associated with a Preferred Camera Server fail back event.

Systems that enforce system-wide settings for failover and fail back operation shall not be acceptable.

1.1 VIDEO ANALYTICS SERVERS

The video analytics (VA) server(s) must be dedicated to analyzing video of interest steamed from the Camera Server(s) only. The VA Server(s) shall not be used to record video footage but shall pass event information from the analysis of the video streams back to the Camera Server(s) supplying the video for analysis for further action.

The VA Server shall:

- Receive live video from Camera Servers
- Process the live video using preconfigured rules and intelligent video content analysis algorithms to determine events of interest
- Transmit intelligent video content analysis event information to the Camera Servers
- Provide video content analysis including:
    - Video Motion Detection
    - Advanced Intelligent Video Content Analysis
    - Provide the ability to monitor cameras for potential tampering including:
    - Changed field of view
    - Blurred image
    - Camera blinded or covered
    - The VA Server shall not be used to record live video or transmit any video – live or recorded – to any other part of the VMS.

The system shall support multiple VA Servers, with no limit to the number of VA Servers use in the VMS.

1.2 OPERATOR STATION

Operator view shall be provided using one or more Operator Station machines. These are connected via a TCP/IP network to the Security, Building control or Industrial control System. They are of capable of viewing live video and recorded video from the Camera Servers. They also provide levels of operator security.

In addition, the VMS shall provide a Microsoft Internet Explorer client interface for viewing and recording live video, video search, replaying recorded video, system configuration and administration.

To aid in software deployment on large systems, the Internet Explorer client shall be able to be installed without the need for external media. The Internet Explorer station shall require n more than a once-off installation of software to the client at the first connection of the client to the VMS web server.

The client shall provide the ability to display up to at least 16 simultaneous video streams in various configurations. It must be possible to support both standard 4:3 aspect ratio screens and wide 16:9 aspect ratio video display monitors without distortion of video but also taking advantage of the entire screen viewing area.

1.3 SYSTEM SIZING

The security system of control system for the site requires that operators be able to simultaneously view record and replay video, as detailed in this specification, for all cameras throughout the sire. The vendor must sixe the Camera Servers to accommodate the live view and recording requirements of the cameras and desired recording setting.

2. HARDWARE

2.1 VIDEO ANALYTIC SERVER

The Video Analytics (VA) Server (when required) shall be able to operate with no performance degradation using the hardware and operating system configuration as specified by the video analytics vendor.

In the event that equivalent hardware is proposed the supplier must be able to demonstrate compatibility of software as described in section 4

Proprietary hardware platforms are not acceptable.

2.2 MULTIPROCESSOR SUPPORT

The VMS server, Camera Server and Video Analytics Server software shall be able to run on both multiple and single processor computers. Where a multiple processor system is used, the VMS software shall be able to make optional use of that configuration.

2.3 SYSTEM FAULT TOLERANCE

A failure of any one of the VMS Servers or Camera Servers shall NOT cause the VMS system to cease operation. As a worst case, only the cameras controlled for by the Camera Server will be unavailable until re-allocated to the other Camera Servers using the VMS software in the event that the Camera Server Redundancy feature is not used. No physical changes to hardware, cabling of connections shall be required.

2.4 OPERATOR INTERFACE

The VMS shall provide 5(five) types of Operators Interface:

- Surveillance Console a dedicated, full feature Surveillance client.

- Integrated Operator Station: A client completely hosted within the Operator Station of the Security system, Integrated Building Management and Control System or Industrial Control system
- Browser client: a light weight Internet Explorer based client.
- Operator Keyboard: A professional CCTV Keyboard interface that allows view and control of cameras without the need for a PC-based Operator Station
- A mobile client supporting Apple and Android iOS-based devices.

PC-based Operator Stations shall provide full control via keyboard and mouse of all parts of the system to which the operator is assigned access. Please refer to the drawing for quantities of each type of Client Machines/ Interfaces.

2.5 SURVEILLANCE CONSOLE

The surveillance console shall provide a dedicated, professional surveillance client used by Security officers. Other clients may be installed and utilized on the physical machine used by the Surveillance Console as required.

The surveillance Console shall have as a minimum the following hardware and Operation System components required to support digital video integration.

- Standard Clients:
  - Inter Core i5-3570 CPU@3.4Ghz or AMD equivalent Hyper threaded
  - 4GB RAM
  - DVD Drive
  - 100/1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card: Any card able to provide a Windows Experience Index subs core of 6.9 or higher (AMD Radeon HD7470 or equivalent)
  - Microsoft Internet Explorer 11
- Performance Clients:
  - Hexa-Core Intel® Xenon® E5-2620 @2.00Ghz or AMD equivalent
  - 4GB RAM
  - DVD Drive
  - 1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card: Any card able to provide a Windows Experience Index subs core of 7.0 or higher (NVIDIA Quadro 4000, Matrox M9140 LP or equivalent)
  - Microsoft Internet Explorer 11
- Ultimate Performance Clients:
  - 2 x Quad-Core Intel® Xenon® CPU X5667 @3.06Ghz or AMD equivalent

  - 4GB RAM
  - DVD Drive
  - 1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card: Any card able to provide a Windows Experience Index subs core of 7.0 or higher (NVIDIA Quadro 4000, Matrox M9140 LP or equivalent)
  - Microsoft Internet Explorer 11

2.6 BROWSER CLIENT

The Browser Client shall support system configuration and casual system viewing.

The Browser Client shall have as a minimum the following hardware and Operating System components required to support digital video integration:

- Standard Clients:
  - Quad-Core Intel Xenon® E5-1620 3.6GHzor AMD equivalent
  - 2GB RAM
  - DVD Drive
  - 100/1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card supporting 24-bit colour and with 256MB on-board video RAM
  - Microsoft Internet Explorer 11
- Performance Clients:
  - Intel® Core i7-3770 3.4Ghz or AMD equivalent
  - 4GB RAM
  - DVD Drive
  - 1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card supporting 24-bit colour and with 1GB on-board video RAM
  - Microsoft Internet Explorer 11
- Ultimate Performance Clients:
  - 2 x Quad-Core Intel® Xenon® W5667 @3.06Ghz or AMD equivalent
  - 4GB RAM
  - DVD Drive
  - 1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card supporting 24-bit colour and with 2GB on-board video RAM
  - Microsoft Internet Explorer 11

Proprietary hardware platforms are not acceptable.

2.7 MOBILE CLIENTS

The VMS shall support mobile clients based on Apple's iOS & Android devices including iPhone and iPad. The app shall be available for download and install from Apple App Store and Android play store. The clients shall support the display of both live and recorded video with the system able to intelligently vary video quality to match the bandwidth available for wireless video transmission.

The mobile client shall support user authentication aligned with the VMS security permissions. Mobile operators shall only be able to see the control cameras to which they have assigned access.

The mobile client shall display a camera tree for easy camera selection. It shall be possible to display multiple cameras simultaneously in live view with up to a 2x3 display for iPhones and iPads. The application shall include a searchable camera tree and list of recently accessed cameras.

It shall be possible to control a PTZ camera directly from the mobile applications. The use shall be able to select configured presets or move the camera via finger press directly on the video footage. Touching the screen above or below the center of the scene shall tilt the camera up or down and touching to the left or right shall pan the image in the same direction. The speed of the pan and tilt shall vary based on the distance from the center of the image to the touch point.

Recorded video shall display as a single camera only and shall include a timeline for display and easy navigation of recordings as well as a date and time selector to quickly locate video. A control shall be provided to support variable speed playback in both forward and reverse directions. An instant replay button shall be provided and shall provide the ability to instantly jump back by a selectable amount of 30 seconds, 60seconds or 5 minutes.

The Mobile Clients shall all support iOS19.x or later and hardware shall be based on:

- iPhone model 5S or later
- iPad Air or later
- iPad Mini with Retina display or later

Mobile video clients that do not support Apple's iOS and Android operating system shall not be acceptable.

2.8 VIDEO WALL CLIENTS

The VMS shall support integration to video wall control devices from at minimum.

The VMS shall support video steaming to the video wall controller by both unicast and multicast streaming. The video wall shall support the configuration of multiple monitors as a single workspace and is shall be possible to command a camera to display on a configured tile in the workspace.

It shall be possible to control PTZ camera displayed on the workspace and direct it to a configured preset, tour or pattern.

2.9 DEVICE SUPPORT: NETWORK CAMERAS AND VIDEO ENCODERS

One instance of Digital Video Management System shall be expandable to support a minimum of 4096 cameras.

The Digital Video Management System shall be capable of supporting up to 150 cameras per Camera Server depending on system configuration.

As a minimum, the system must support network cameras and video encoding devices:

- Network Video Encoders:
- Network Cameras:

The VMS shall support at least industry-standard Motion IPEG and H.264 encoding formats.

The VMS shall support certified ONVIF devices that conform to the ONVIF Profile S and Profile G standard. The VMS shall be a certified ONVIF Network Video Client with certification for both ONVIF Profile S and Profile G registered on the ONVIF website as minimum requirements. Systems that do no support ONVIF Profile S and Profile G will not be acceptable.

The VMS shall support the ability to analyze and upload device capabilities of supported manufacturers ONVIF complaint devices. Once discovered, device details shall be added the VMS database and used for further device configuration. System that requires a software update to add support for new devices from supported manufacturers shall not be acceptable.

3. SYSTEM SOFTWARE

This section describes the required System Software. If other software is proposed they suppliers must be able to demonstrate full compliance with Section 4.

The proposed solution shall be based on standard Microsoft technology for Server and Client/desktop Operating System and Database solution.

4. APPLICATION SOFTWARE FUNCTIONS

4.1 SURVEILLANCE CLIENT OPERATION

Operators shall utilize one or more of the available VMS Client interfaces depending on their specific operation role and needs.

4.1.1 SURVEILLANCECONSOLE

The Surveillance Console shall provide a professional level surveillance interface for control room operators. Its primary role shall be to meet the operational requirements related to surveillance.

The Surveillance Console shall inherit Security permissions from the Security System, Integrated Building Management and Control System or Industrial Control System. Security shall be managed by the use of Trusted Root Certificates which will allow the Surveillance Console to communicate with the required Database and Camera Servers.

Solutions that do not allow for integration of the Security model between VMS and the Security System, Integrated Building Management and Control System or Industrial Control System shall not be permitted.

The Surveillance Console user interface shall consist of the following key elements:

- Navigation Pane.
- Flexible Video Workspace
- Timeline with video Export capability
- Recently Used Camera List

It shall be possible to minimize each individual element of the Surveillance Console to maximize the use of the screen for video display.

The Surveillance Console Client shall be configurable with both dark and light themes to assist with usability in light or dark control room environments.

The individual elements of the User Interface shall operate as follows:

4.1.1.1 Navigation Pane

The Navigation Pane shall include separate tabs to display available cameras, Views, groups and location available to the operator base on their security settings. It shall include a Camera Tree as well as a location for defining logical groups of elements.

The Camera Tree shall be a multi-level element up to at least 5 layers deep and shall display cameras, groups and predefined camera views as separate icons.

The Camera Tree shall conform to the system security model and only allow operators to see and interact with devices to which they have been provided rights.

It shall be possible to arrange cameras in locations on the Camera Tree, either by via integration with the facility model of the Security System, Integrated Building Management and Control System or Industrial Control System or by manually creating groups and allocating applicable cameras.

The Camera Tree shall provide a location for operators to create their own logical groups of cameras to suit their individual operational surveillance needs. Cameras and Views shall be able to appear in multiple logical groups.

The Camera Tree shall include an automatic filtering facility which allows for dynamic filtering of the items in the tree as text is typed into the filter text box. Searchable items shall include cameras, locations, multi-camera views and bookmark text.

It shall be possible to drag individual cameras, locations, groups or Views to the Video Workspace to display all cameras involved in the operation. Cameras shall also be added to the workspace by a single left mouse click – which will add the camera to the next empty tile – or by double –clicking the left mouse button – which replaces the existing selected Tile's camera with the new camera.

Double left-clicking on a group or location will replace all cameras in the Workspace with the new Group or Location. Single left-clicking on a Group or Location will expand or collapse the Group or Location in the Navigation Pane.

4.1.1.2Flexible Video Workspace

The Video Workspace shall display cameras in 1 or more tiles and it shall be possible to arrange the Video Workspace into a number of different layouts. The layouts shall be selectable from a list of options displayed as icons on the Video Workspace toolbar providing a visual representation of the layout. Separate layouts shall be provided 4:3 and 16:9 aspect ratio monitors.

Tiles in the Video Workspace shall display either a single camera or cycle through multiple cameras. A header bar shall be provided in the Workspace to indicate information about a current View being displayed or to control the cycling of cameras in the workspace.

Tile shall display either Live or Recorded video. The Video Workspace shall support the simultaneous display of Live and Recorded video from the same or different cameras. Information describing the camera and associated video shall be shown in the tile including camera name, camera number, camera health status and whether the camera is currently recording, replaying video, pause or playing live video.

The tile shall provide a tile toolbar which appears as a popup when the mouse pointer is hovered over the tile. The toolbar shall provide buttons to allow interaction and control of the camera directly. Buttons shall include at least: instant playback, return to live, record, snapshot, playback controls, focus, iris, digital zoom, preset controls and annotation controls.

It shall possible to control PTZ cameras directly from the Tile in the Workspace. Control shall be either via the controls on the popup overlay menu or by clicking directly on the video in the tile.

It shall be possible to drag on or more selected cameras between tiles to allow rearranging of the camera in the Workspace as required by the operator.

All cameras dragged from a location on Navigation Pane shall be displayed in the Workspace. In the event that the number of cameras dragged into the Workspace exceeds the number of available tiles, the additional cameras will cycle in tiles on the Workspace.

It shall be possible to clear the workspace via a single operation by clicking a button on the Workspace toolbar.

It shall be possible to maximize the workspace to the full screen mode, whereby the Workspace shall expand to fill the entire monitor screen.

The Workspace toolbar shall include a keyboard command box that allows for typed commands to be entered and executed. Keyboard commands shall include:

- Arrows: move selection between tiles
- CTRL+A: Select all cameras in a Workspace
- F11: Switch to Full Screen mode (and ESC to cancel)
- Enter: maximize/minimize the tile with focus
- Delete: remove the selected cameras from the workspace

Integration with Security System, Integrated Building Management and Control System or Industrial Control System shall provide the ability to create custom display pages within those systems with embedded camera objects from the VMS. It shall be possible to drag those camera objects to the VMS Surveillance Client Video Workspace and hence display that camera in a Tile on the Workspace.

4.1.1.3 Timeline

The Surveillance Client shall provide a timeline control to display and play back recorded video for one or more cameras. Playback shall be possible on 1 or more cameras simultaneously for all cameras currently displayed in the Video Workspace.

Each cameras and its associated recording shall be represented in the timeline by a separate row. Background and Scheduled Recordings shall be represented as thick horizontal rows in the camera row while other recording types shall be represented as thinner, vertical lines.

The Timeline shall provide a play head control to indicate the time of the recoding currently viewed for all cameras in the timeline. The play head shall also be used to scrub through video for all recordings in the timeline.

A Timeline toolbar shall be provided to assist with playback of recordings. The toolbar shall include the following standard features as a minimum:

- Play: play recorded video

- Pause: Pause video currently being played
- Snapshot: Captures a single frame of video from the current scene
- Fast rewind: rewinds the video at a speed related to the number of times the button is clicked with each click increasing the rewind speed by a factor of 4 from 4 times to 1024 times normal speed. Clicking once rewinds the video at normal speed with subsequent clicks increasing the speed. Video speed shall be slowed by right-clicking one or more times with each right-click reversing the speed by a single factor of 4. Right-clicking when displaying normal speed will slow the replay to 0.75, 0.5 and 0.25 normal speed on respective clicks. The fast rewind operation shall be applicable to all cameras displayed in the timeline.
- Frame rewind: Rewinds the video a single frame per click or click and hold to rewind continuously through individual frames
- Frame Forward: Advances the video a single frame per click or click and hold to rewind continuously through individual frames
- Fast Forward: plays the video at a speed related to the number of times the button is clicked with each click increasing the speedby a factor of 4 from 4 times to 1024 times normal speed. Video speed shall be slowed by right-clicking one or more times with each right-click reversing the speed by a single factor of 4. Right-clicking when displaying normal speed will slow the replay to 0.75, 0.5 and 0.25 normal speed on respective clicks. The fast forward operation shall be applicable to all cameras displayed in the timeline.
- Jump Back: Control containing 3 separate buttons to rewind and start playing video for 30 seconds, 1 minute and 5 minutes prior to that point in time.
- Motion Search: Enables the Motion Search operation which allows configuration of the parameters to search for motion in recoded video.
- Regions of Interest: This option shall be displayed if live video annotations are enabled. Selecting the option shall show or hide the configured regions of interest.
- Calendar control: allows the ability to select a date and time to which to navigate immediately.
- Video Export; allows operator the ability to select export duration on one (1) or more cameras directly from the timeline and export them in a single operation as per section “Video as evidence Digitally Signed Recordings and Audit Logs”

It shall be possible to ass any camera currently displayed in the Video workspace to the timeline allowing the timeline to contain from 1 up to the total number of cameras displayed in the Video Workspace. It shall be possible to replay 2 of more videos displayed in the timeline in time synchronized playback.

It shall be possible to add any camera visible to the operator to the timeline by a simple drag- & - drop operation from both camera tree and the video workspace.

The timeline shall provide a Motion Search feature that allows searching for areas of motion in recorded video. The Motion Search feature shall provide the ability to define a region of interest for each camera currently included in the timeline. The region of interest will be displayed on the camera image in the Video Workspace and each shall be separately configurable.

Motion Search shall commence from the position of the play head on the timeline and an indication shall be provided on the corresponding tiles in theVideo Workspace that motion search is in progress.

Motion results shall be indicated on the camera rows in the Timeline as discovered and it shall be possible to navigate to each event via “Next Event” and “Previous Event” buttons. Video can be replayed at these events while motion search is currently active.

It shall be possible to stop or disable motion search as required.

It shall be possible for operators to add bookmarks to video directly from the timeline. A button shall be provided for this purpose and shall allow the operator to insert the bookmark at the point of the play head position one pressed. Bookmarks must be associated with recorded video and shall be visible to all users.

Bookmarks shall by default be added to all cameras present in the timeline. It shall be possible to deselect bookmarks if not required on specific cameras at the point of creation.

Bookmarks shall be represented on the timeline to allow easy identification. Selecting a bookmark shall display the text entered by the operator.

It shall be possible to modify to delete bookmarksprovided the user has the appropriate security permissions.

Bookmark text shall be a searchable item in the VMS camera tree. Selecting the bookmark found or dragging the bookmark to the video workspace or timeline shall load the camera recording and automatically locate the play head to the frame closest to the bookmark location automatically.

It shall be possible to easily navigate between bookmarks on a camera by using a “Jump to Next” feature included on the timeline.

4.1.1.4 Recently Used Camera List

The Surveillance Console shall provide a visual location for cameras that have recently been viewed by the operator. Camera displayed in this location shall be represented by a live view image from the camera at reduced frame rate for easy reference.

Cameras shall be displayed in the recently used list under the following scenarios:

- They are removed from a tile and are not shown in any other tile in the Video Workspace.
- They are replaced in the Video Workspace due to a layout change.
- The camera was part of a cycling view of cycling camera tiles when the Video Workspace was altered and the camera no longer fits on the Video Workspace. A Video Workspace can be altered by selecting a different workspace layout or cameras being added or removed on the Video Workspace.

It shall be possible to select and move a camera from the Recently Used List to the Video Workspace for further viewing.

It shall be possible to display a minimum of ten (10) cameras in the Recently Used List.

It shall be possible to clear a single camera or all cameras displayed in the Recently Used List.

4.1.2 INTEGRATED OPERATOR STATION AND BROWSER CLIENTS

For the purpose of this section, Integrated Operator Station Clients and Browser Clients shall be handled together as their operational functionality is equivalent.

The live output from cameras shall be configured and viewed through a series of displays. These shall support:

- Single camera view
- Multiple camera viewing of up to 16 cameras simultaneously, each at 25/30fbs and each vies port supporting sequencing of cameras and/or cameras presets for PTZ cameras
- Specific viewing options for both standard aspect ratio as well as wide aspect ratio (wide screen) monitors thus preventing distortion of original video aspect ratio while still taking advantage of the entire screen area for image display of multiple video channels.
- Sequence view of camera preset positions
- Modifying settings for a camera
- Modify recording settings for a camera
- Adding and deleting cameras
- Creating schedules for recordings, video analytics and Input/output monitoring and switching
- Modifying Video Analytics settings and tuning for:
    - Video Motion Detection
    - Object Tracking
    - Object Classification
    - Intelligent Video Analytics

- Modify settings for Inputs and Outputs on IP cameras and video encoders
- Modify settings for camera tamper detection
- View and initiate Intercom calls with cameras configured with bi-directional audio capabilities.

Users shall be able to select a camera from a tree control listing the cameras available to the user.

4.1.3SINGLE CAMERA

From this display, the user shall be able to:

- View the live output from the selected camera
- Pan, tilt, zoom and focus the camera using a pointing device attached to the Operator Station PC. Standard Microsoft Windows supported pointing devices such as a mouse or touch-screen shall be supported.
- For cameras which support continuous pan, tilt, zoom (PTZ), a mouse shall be able to be used for continuous PTZ directly in the live video window. By dragging the mouse up or down, left or right in the video window, the operator shall be able to tilt the camera up or down, or pan the camera left or right. Zooming must also be provided using the mouse in a similar way.
- Manually record live video, Recording will continue for the configured period of time. Once recording has begun, a stop button shall be provided as well as a counter showing the recoding time remaining.
- Manually store the current frame of video (snapshot) as bitmap image file. The file name shall be automatically generated by the VMS software and include the camera name, date and time of the recording (to millisecond precision).
- Indicate whether video motion detection is currently enabled for the selected camera.
- Digitally zoom into a region of the image
- Enhance the image by adjusting brightness, contrast, noise levels of sharpness of the image.

4.1.4 MULTIPLE CAMERA VIEWS

The VMS shall support multiple camera views. A multiple camera view consists of up to sixteen related cameras viewed simultaneously on a single display.

The layout for a view shall be configurable from a selection of different layouts templates. There shall be a set of templates for standard aspect ratio (4:3) monitors and another set of templates for side aspect ratio monitors to properly utilize the entire monitor screen real estate without distorting the original video aspect ratio.

It shall be possible to configure and save individual views for re-use. It shall be possible for the view to be created by dragging and dropping cameras and presets if applicable directly into the view ports from the camera tree.

Standard aspect ratio templates shall include:

Single camera (sequencing –see 4.1.4.1)

- 2 x 2 View
- 3 x 3 View
- 4 x 4 View
- 1 + 5 View
- 2 + 8 View
- 1 + 12 View

Wide aspect ratio templates shall include:

- Single camera (sequencing –see 4.1.4.1)
- 2 x 3 view
- 3 x 4 View
- 1 + 3 View
- 2 + 4 View
- 1 + 8 View

Multiple camera views shall be divided into quadrants. For each quadrant the view shall have a camera or be blank. Within each quadrant the view shall be configured to cycle between any of the cameras accessible to the user on a configurable time basis. Pan-tilt-zoom cameras, which support preset positions, can have these presets cycled on a time basis. In this way an operator can view a variety of presets on a series of PTZ cameras in a multiple camera view.

It shall be possible to show the camera names of each camera and preset (if applicable) configured in a view on either the operator station and on surveillance monitors. Hovering the mouse pointer over a view port shall trigger a tooltip showing the camera name and preset (If applicable).

There shall be no limit to the number if cameras that can be assigned to a single multiple cameras view. There shall also be no limit ot the number of available multiple camera views.

The system shall support the ability to intelligently manage video streaming to the alarm and spot display monitors by automatically selecting a lower quality video stream when displaying multiple cameras on a single stream. The quality of the video stream for this purpose shall be configurable on a per-camera basis. The system shall automatically switch between the lower quality stream (if configured) and the normal live video stream when switching from a multi-camera view to a single camera view.

4.1.4.1 Sequence view

The VMS shall support sequence views. A sequence vies consists of a single camera view, which can be cycled on a time basis. Pan-tilt-zoom cameras, which support preset positions, can have these presets cycled on a time basis. In this way an operator can view a variety of presets on a series of PTZ cameras. Fixed cameras can also be included in the sequence and cycled accordingly.

There shall be no limit to the number of cameras that can be assigned to a single Sequence View. There shall be no limit to the number of available Sequence Views.

4.1.5 VEIEWING OF RECORDINGS

The recorded video shall be available to all users, which have adequate security. Each user shall only be able to view recordings from cameras they have security access to view.

A display shall be provided to view recordings from any Operator Station. From this display, the operator can select the recording he/she wishes to view, which shall be immediately shown in an embedded video player.

The following information and controls shall be provided on this display:

- A navigation panel to allow the user to select the required camera
- A calendar control (similar to Microsoft Outlook) to select the desired date. All days which have recordings for the chosen camera shall be displayed in bold font.
- A table listing all the recordings on the chosen camera for the chosen day. The user shall be able to select the required recording from this table. Each column shall be able to be sorted by selecting the column heading. This table shall display the following information as a minimum.
- The time each recording was activated
- The duration of each recording
- The type of recording (operator, event, video analytics, camera tamper, input/output scheduled or background)
- The Operator or user that activated the recording (for operator activated recordings)
- The Name, Description and Value of the Security System Server or Control System Server which activated the recording (for alarm/event activated recordings)
- An embedded video player with controls (buttons) similar toa VCR (video cassette recorder). The information displayed on the video player and the controls provided shall include:
- The time and date of the frame being displayed
- A slider control which is used to move backwards and forwards through the recording
- Play, pause and stop buttons
- Step forward and rewind buttons, to play the recording at speed s of x2, x4, x8, x16, etc (to a minimum of x 1024). Video speed shall be slowed by right-clicking one more time

with each right-clicking reversing the speed by a single factor of 4. Right-clicking when displaying normal speed will slow the replay to 0.75, 0.5 and 0.25 normal speed on respective clicks.

- A snapshot button, to allow for the frame being displayed being stored as a bitmap file (in a similar way to the snapshot button for live video).
- Buttons to access slider bars for adjusting the brightness, contrast, noise levels and sharpness of the image
- A mouse-pointer activated overlay allowing for control of digital zoom.
- Information about the chosen recording. The following information as a minimum shall be displayed with the chosen recording
- The sub-priority of the recording (for alarm/event activated recordings)
- The frame rate the recording was recorded at
- The resolution of the recording
- The compression used
- The recording start time and date (including pre-record)
- The recording end time and date
- The date and time that the recording will be deleted by default (which can be changed as required)
- Operator comments and notes about the recording (made by the scheduled recording configuration automatically or by an operator)
- The date and time that the recording will be archived by default (which can be changed as required)
- The date and time that the recording will be deleted by default (which can be changed as required)
- When a recording is displayed, the exact frame of video when the recording was activated shall be shown. The slider shall be positioned accordingly along with the frame time. It is not appropriate to show the first frame in the recording, as the recording may have pre-event recording.
- Buttons to allow the operator to archive, delete or export the chosen recording
- A button is provided to playback the recording at the recorded resolution. This shall be done using a display that pops up containing the embedded video control with full playback functionality as described above.

4.1.6 SEARCHING FOR RECORDED VIDEO

4.1.6.1 Simple Search

The VMS shall provide a simple search for all video recorded. The user selects the time indicator which shows a Calendar and time line. The user selects the required search period.

Once the time criterion is entered, the “search” is selected. Video recorded during the selected period will be returned by the search.

The user shall be able to search on combinations of cameras by clicking on an “Advanced Search” icon as described in the next section.

4.1.6.2 Advanced Search

The VMS shall provide an advanced search of recorded video. The search shall be based on recording time, camera and recording details.

The user shall select from the list of cameras. It shall also include any cameras that have been deleted from the system but still have video stored on a Camera Server or on archived media. If a camera has been deleted and all video associated with the camera has been deleted, the camera will not appear in this list.

The time criterion shall be selected from a calendar and time line control, Days containing recorded video shall be shown in bold on the calendar control. Cameras shall be able to be added and removed from the search list.

The user shall be able to choose to filter the search based on the following criteria:

Alarm if event type of alarm/event activated recordings

Recording type (operator, event, video analytics, camera tamper, input/output scheduled or background)

Area

Point name

Event description (urgent, high, low, journal and all)

Operator name

Camera name or number

Any comments entered by users in the comments field of recordings

Wildcards shall be accepted for the Point ID, description, area priority and value for alarm/event activated recordings.

4.1.6.3 Search results

The VMS shall show the results of the basic and advanced searches in a table format, such that the user is able to select column within the list to sort the output. Functionality shall be provided to allow the user to see a list of recordings for a camera from the past 24 hours without needing to use on of the searches.

4.1.7 VIDEO AS EVIDENCE: DIGITALLY SIGNED RECORDINGS AND AUDIT LOGS

Export of video for evidentiary purposes shall be possible directly from the Operator Client. Systems that require a separate application to manage video export shall not be acceptable.

The VMS shall support at minimum two means for video authentication:

- Digital Signature: A default Digital Certificate shall be provided and installed on Client computers used for Export purposes. It shall be possible to utilize digital certificates purchased from the other certificate authorities as required and supported by corporate policy.
- Water marking: a default water mark image shall be provided and it shall also be possible to configure a custom image as a watermark. It shall be possible to configure the size and location of the watermark in the exported video as a its opacity.

It shall be possible to select the portion of video require and export only that portion.

It shall be possible to select the video to be exported directly from the video timeline in the Operator Client. Manipulation of the export range for each camera shall be performed using the mouse and allow dragging of the export range and it edges to select the desired period for each camera. It shall be possibleto configure unique time periods for each camera in the export operation.

It shall be possible to export video from 1 or more cameras in a single operation from the timeline. The maximum number of cameras managed in a single export shall be limited to the number of cameras displayed simultaneously in the operator’s video workspace.

The user will be able to optionally export a recording in the original, native video format, which will keep the original video format unchanged. It shall be possible to select either Windows Media Format (default) or Native Format when exporting video.

- Windows Media Format: the exported video will be transcoded using the Windows Media Video codec. The exported video file will have the .wmv extension.
- Native Format: the exported video will not be transcoded and will remain unchanged. The exported video file will have the .asf file extension.

System that require a proprietary viewer application for viewing exported video shall not be acceptable.

The system shall provide the ability to export the system event log associated to the export range along with the video.

The system shall provide the ability to overlay the camera and recording date and time details on the exported video. It shall be possible to enable and disable this feature at the point of export as required.

It shall be possible to select the export destination location and provide a unique name for the export.

The system shall provide visual feedback as to the progress of each individual camera's export status as well as the overall video export progress and status. This feedback will include estimated remaining duration of the export action and size of the export package. This feedback shall also include any errors or warnings associated with the export operation. The system shall provide the ability to cancel the entire export or remove individual cameras from the export operation without disrupting the export for the remaining cameras.

The Operator Client shall create a queue of recordings to be exported and shall allow items to be exported concurrently where possible. Client CPU utilization shall be monitored during the export process and the export load adapted to ensure that the Operator Client PC CPU utilization remains below 90%.

The VMS shall allow for the protection of the exported video by means of a freely configurable password for each package.

It is a requirement for all exported recordings and exported audit logs to be digitally signed. This require to prove authentication (origin of the recording and audit log)and integrity (exported recording and audit log have not been altered of tampered with).

The VMS system shall provide a default digital certificate for signing the exported recordings and audit logs. Customization shall also be provided to allow the user to supply his/her own digital certificate.

A utility shall be provided to display the exported recording, view the audit log and verify the digital signatures. A visual indication shall be provided to whether the exported recording and audit log have been altered or tampered with.

4.2 ALARM AND SPOT MONITORS

The system shall also support the display of video on spot and alarm monitors in the following manner:

- Alarm monitor: when an alarm occurs in the Security System, Integrated Building Management and Control System of Industrial Control System Server, the live video output associated with that alarm shall be switched directly to an alarm monitor. The system shall support the switching of both live video from single cameras as well as from a collection of cameras associated with the alarm. The use shall be able to acknowledge the alarm monitors will not be removed from the queue unless explicitly cleared by the operator. It shall be possible to create a queue of alarm monitors to manage multiple alarm views simultaneously.

- Surveillance Monitor: Operators shall be able to call up both single camera views and multiple camera views to a surveillance monitor. It shall be possible to sequence the cameras displayed on the surveillance monitor and the system shall support sequences of single camera as well as cameras sequencing in individual view ports when a surveillance monitor displays multiple cameras simultaneously. The user shall be able to clear the monitor using the numeric keyboard. It shall be possible to call cycle up a camera to an individual tile of a multiple camera view displayed on Surveillance Monitor.
  Monitors shall be able to be configured to act as both Alarm and Surveillance monitors. In this case, the monitor behaves as a Surveillance monitor until an alarm occurs, in which case it shall show the alarm video. Once the alarm is acknowledged, the video previously shown(as a surveillance monitor) is displayed again.
  In each of these cases, these additional monitors shall be either connected to an Operator Station using a multi-monitor PC card or to other PCs.
  The system shall support the ability to intelligently manage video streaming to the display monitors by automatically selecting a lower quality video stream when displaying multiple cameras on a single stream. The quality of the video stream for this purpose shall be configurable on a per-camera basis. This system shall automatically switch between the lower quality stream (if configured) and the normal live video stream when switching from a multi-camera view to a single camera view.
  Systems that do not offer this functionality will be disqualified.

4.3 VIDEO LOSS ALARM

The VMs shall support the video encoder Video Loss Alarm feature. The Video Loss Alarm feature shall provide VMs operators with a notification when the video signal from the camera to the video encoder is lost. A video loss alarm shall result in an alarm being raised, the change of the camera icon in the camera tree to indicate the alarm condition and an entry in the system audit log for future reference,

4.4 CAMERA TAMPER DETECTION

The VMS shall provide the ability to detect attempts to tamper with connected cameras. The system will at minimum detect the following:

- Changed field of view: repositioning the camera away from a reference position shall trigger an alarm.
- Camera blur: any attempt to defocus or blur the camera shall trigger an alarm.
- Camera blind: any attempt to cover or blind the camera (via abnormally high light levels) shall trigger an alarm.

Each of the above options shall be individually selectable as required per camera. It shall thus be possible to enable any combination of the above three detection options on each camera connected to the VMS.

The detection algorithms for tampering shall e run on one or more of the VMS Camera Servers. It shall be possible to configure and tune the algorithms individually per camera. The configuration screen shall provide:

- The ability to enable any combination of the tamper detection algorithms
- Real time feedback of the percentage of tampering detected
- The ability to set the threshold at which a tamper alarm will be generated
- Real time feedback of when a tamper threshold has been crossed
- How often the detection algorithm should check for a tamper condition
- Systems response to a tamper alarm including:

- Starting a recording with the possibility of also configuring the system to record video prior to the event occurring. It must be possible to record video prior to the event occurring where the duration this pre-record is a pre-configured value.
- Generating alarms with configurable alarm levels
- Sending live video to an Integrated Operator Station
- Trigger an output on a device connected to the VMs such as a network camera or video encoder.

Once a tamper condition is detected, the system shall provide visual indication to the operator through both a text overlay on the live video and indication on the camera tree. The text overlay shall be for viewing purposes only and shall not be recorded.

Systems that provide the same camera tamper settings for all cameras shall not be acceptable.

4.5 CAMERA SETTINGS

Camera configuration shall be accomplished via the Integrated Operator Station or Browser Clients.

Users shall be able to change important settings for an individual camera from the local system to which that camera is assigned. The details are grouped into several sections:

- Camera Details
- Camera Connection
- Camera PTZ Control
- Security
- Camera Deletion

The parameters listed in the sub-sections below are configurable on a per camera basis and their specific selection on a particular camera(s) will not limit the ability to freely select other options on other cameras as required. It will be easy to change any of these parameters for each camera individually as and when required. Systems that do not allow changes to each camera's parameters on an individual basis will not be acceptable.

Only users with the highest level of security are permitted to modify camera connection details, camera PTZ control or delete cameras.

4.5.1CAMERA DETAILS

The user shall be able to configure the following parameters for each camera:

- Camera name
- Allocated Camera Server
- Location
- Description
- Camera Number (for fast numeric keypad call-up)

4.5.2CAMERA CONNECTION

The VMS shall provide the capability to define the connection parameters for each camera and include the following items:

- Camera Family and Model
- Camera IP address
- The frame delivery type, unicast or multicast
- The stream type video, video and audio or video and bi-directional audio
- The video format: PAL or NTSC

It shall be possible to configure unique video stream profiles for each camera. The system shall support up to 4 unique stream profiles, depending on the capabilities of the IP Camera of video encoder used.

It shall be possible to defined the priority of the different video stream profiles configured for each camera.

Each stream profile shall be comprised of the following parameters:

- User-configurable name
- Compression format H.264, MPEG4 or Motion JPEG
- Stream limiter type: Stream limited by either frame rate or bandwidth
- Steam limit: Frame Rate of Bandwidth value

- GOP (MPEG4/H.264 only)
- Video Resolution
- Video Compression ratio

Each stream profile shall be assignable as follows:

- Live video display (all clients except Mobile)
- Mobile Clients
- Low resolution profile (for use with multi-camera views)
- Supported recording types

4.5.3 CAMERA CONTROL

The user shall be able to configure any appropriate camera to be PTZ controllable.

The following camera types must be supported as a minimum:

- Video Controls Limited (VCL) Orbiter cameras
- Honeywell Video Rapid Dome cameras
- Cameras supporting the Pelco P protocol
- Cameras supporting the Pelco D protocol
- American-Dynamics Speed Dome
- Honeywell HVE video encoder series supported PTZ cameras and device

The following PTs characteristics shall be tunable on a camera-by-camera basis from the cameradefinition pages:

- Pan Speed
- Tilt Speed
- Zoom Speed
- Focus Speed
- Iris speed
- Increment step size
- Continuous Pan/Tilt Speed

The VMS shall provide the ability support streamer-side camera control for video encoding devices providing this feature. In this case, the video encoding device will be responsible for providing the control mechanism to the associated camera and the communications protocol will not need to be natively supported in the VMS.

4.5.3.1 Advanced Camera Control

The VMS shall provide more advanced control capability for cameras supporting the Pelco D Camera protocol as well as the features mentioned below. The VMS shall support the following Functions:

- Control of the camera washer and wiper function via dedicated button on the VMS User Interface. A hardware interface via the output port of a video encoding device shall not be sufficient.
- Call up and navigation of the device system menu and setting of device options on this menu via the VMS User Interface.
- The ability to record patterns of motion for a Pan/Tilt/Zoom camera. These patterns will be available as preset positions for Pan/Tilt/Zoom cameras allowing the cameras to “patrol” the facility when not being controlled by operators.

The VMs shall provide access to the absolute positioning coordinates of Pan/Tilt/Zoom cameras using the Pelco D protocol. The coordinates will be provided via the VMs Application Programming Interface – see section 4.16 (system diagnostics)

4.5.4 SECURITY

The following parameters shall be configurable for each camera:

- Area: Allows the system to be configured to only allow user to view specified cameras. These areas shall be the defined by the Security System, Building Control System or the Industrial Control System
- Control Level: Determines if a user is allowed to operate the PTZ controls for a camera. Also used to allow higher-level users to take control of cameras. These Control Levels shall be defined by the Security System, Building Control System or the Industrial Control System
- Control Reservation Period: Once a particular user has controlled the camera no other user can control the camera until this reservation period has expired. Users with higher security level shall be able to take control of the camera at any time.

4.5.5 CAMERA DELETION

The “Delete” function shall allow a user with the highest-level security to delete the camera from the system. After deletion name of the camera will no longer appear in the list of cameras. All camera settings will be deleted but the camera record will remain in the database for searching purposes.

Any recordings associated with a deleted camera will remain until their configured deletion date. The recordings will remain on the Camera Server and archive media unless they are later individually deleted. The camera name will also continue to appear in the list of cameras used for searching the video clip database.

4.6 RECORDING VIDEO

Recorded video will be stored by the Camera Server in one of the following locations:

- Internal hard disk drive array

- External, direct attached storage array
- Network storage location

The Operator station shall be able to locate relevant recorded video and to then replay that video at the Operator Station.

The VMS shall support the replay of recorded video from any location provided the recording can be accessed by a functioning Camera Server deployed on the system. Recording playback shall not be affected by the availability of the original recording Camera Server.

The system shall provide the ability to use any of the defined video stream profiles – as define in section 4.5.2 – for the device for recording purposes. All recording types shall use the same video encoding format.

The system shall only record a single video stream from each camera configured in the system so that most efficient use is made of available system storage. If more than one (1) recording type is active simultaneously, the systems shall record the video delivered by the video stream profile with the highest defined priority.

The following methods of recoding live video shall be supported:

- User activated
- Event activated by the Security System, Building Control System or the Industrial Control System
- Streamer and/or IP camera Inputs/Outputs
- Scheduled
- Continuous background recording
- Video Analytics
- Video Motion Detection
- Intelligent Video Analytics
- Camera Tamper events
    - Snapshot
    - PTZ – Activated
    - Edge Recording

4.6.1 USER ACTIVATED RECORDING

User activated recording occurs when a user viewing live video chooses to record the currently viewed camera output by selecting the “Record” button on the applicable user interface.

The user shall be able to configure the following parameters uniquely for each camera:

- Pre-Record Duration: The amount of pre-recorded video that will be associated with a user request for recorded video. This will allow the Camera Server to capture video prior to the user request, as well as after the request. Shall be selectable from a list of values ranging from No Recording to 5 minutes.

- Frame Rate: Video quality required for user activatedrecording. It shall be possible to have different frame rates for user and event-activated recordings. Shall be selectable from the entire range of frame rates supported for the camera. For MPEG encoding (including H.264), support shall also be provided to record only the Index frames, or a subset of the Index frames.
- Record Duration: user activated recordings shall terminate after this period. Shall be selectable from a list of values ranging between 0 seconds to 10 minutes.
- Retention Period: The default period that the Camera Server shall retain user-activated recordings before being deleted. The retention period of individual recordings shall be able to be changed on a per-recording basis. Shall be selectable from a list of values ranging between one hour and forever.
- Archive After period: The default period for which user activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- Delete After period: The default period that the recording will be retained before being automatically deleted by the system. The Delete After period ofindividual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

4.6.2 EVENT ACTIVATE RECORDING

Event activated recording is a process that allows a segment of video or a snapshot to be associated with the Security System, Building Control System of Industrial Control system alarm or event.

There shall be at least four priorities of alarms/events in the Security or Control System

- Event (journal priority)
- Low priority alarms
- High priority alarms
- Urgent priority alarms

The following settings shall be individually configurable for each alarm and each camera:

- Pre-Record Duration: The amount of pre-recorded video that will be associated with an alarm/event, as well as after the alarm/event. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
- Post Record Duration: Event activated recordings shall terminate after this period.Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
- Frame Rate: Video quality required for event activated recording. It shall be possible to have different frame rates for user, event-activated, scheduled and motion detection activated recordings. Shall be selectable from the entire range of frame rates supported for the camera/streamer. For MPEG encoding (including H.264), support shall also be provided to record only the Index frames, or a subset of the Index frames.
- Retention Period: The default period the Camera Server will retain event-activated recordings before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.
- Archive After period: The default period for which event activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip’s end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- Delete After period: The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip’s end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

The pre-record and post-record durations in the paragraph above define the maximum allowable limits for each camera. They shall be configured on a camera-by-camera basis. However each alarm or event causing video to be recorded shall also be capable of individual configuration with pre and post alarm periods being selected from a range defined by the maximum settings for the camera.

VMS systems requiring a single pre and post record event period to be defined for all alarms and events on an individual camera are not acceptable. VMS systems requiring a single pre and post event period to be defined for all alarms and events on all cameras are also not acceptable.

In the case of multiple alarms/events relating to the same camera, a video clip shall be created for each alarm/event.

For cameras that support Pan/Tilt/Zoom and Presets, a specified preset location shall be selected automatically when the alarm/event occurs prior to the event activated recording commencing. For example, when an alarm is detected on a security door, the alarm shall trigger a PTZ camera to move to a preset position, which is pointing at the door prior to the VMS commencing recording.

4.6.3 DEVICE INPUT/OUTPUT ACTIVATED RECORDING

Input of output recording activation occurs when an input or an output connected to an IP camera or steamer is activated and then subsequently triggers recording on one or more associated cameras.

It shall be possible for any digital input or output connected to a steamer or IP camera on the system to trigger a recording on one or more cameras simultaneously.

The following settings shall be individually configurable for each alarm and each camera:

- Pre-Record Duration: The amount of pre-recorded video that will be associated with a device input/output. This shall allow the Camera Server to capture video prior to the alarm/event, as well as after the alarm/event. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
- Post Record Duration: Device input/output activated recordings shall terminate after this period.Shall be selectable from a list of values ranging between 0 seconds and 10 minutes or while the device is active.
- Frame Rate: Video quality required for device input/output activated recording. It shall be possible to have different frame rates for user, device input/output activated, event-activated, scheduled and motion detection activated recordings. Shall be selectable from the entire range of frame rates supported for the camera/streamer. For MPEG encoding (including H.264), support shall also be provided to record only the Index frames, or a subset of the Index frames.
- Retention Period: The default period the Camera Server will retain deviceinput/output activated recordings before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.
- Archive After period: The default period for which deviceinput/output activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip’s end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- Delete After period: The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip’s end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a

default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

The pre-record and post-record durations in the paragraph above define the maximum allowable limits for each camera. They shall be configured on a camera-by-camera basis.

For cameras that support Pan/Tilt/Zoom and Presets, a specified preset location shall be selected automatically when the input/output event occurs prior to the recording commencing. For example, when an intrusion alarm is detected, the alarm shall trigger a PTZ camera to move to a preset position, which is pointing at the area monitored by the intrusion sensor prior to the VMS commencing recording.

4.6.4 SCHEDULED RECORDING

Scheduled recording allows video to be recorded between start and stop times on defined days.

The system shall support the ability to schedule recordings for each individual camera for times in the future. For each scheduled recording the user shall be able to configure the following (with descriptions as per User Activated and Event Activated recordings):

- Start time
- Stop time
- Frame rate for the recording
- Retention period before the recording will be deleted
- Recurrence (if this is to be a recurring schedule)
- Description (at least 255 characters)
- Archive After period providing the period after which the recording will automatically deleted
- Whether audio is recorded with the scheduled recording or not (if supported on the camera)

There shall be no limit on the number of schedules that can be entered fir the system. There shall be no limit on the number of schedules per camera.

4.6.5 CONTINUOUS BACKGROUND RECORDING

The system shall support the ability to provide continuous background recording from any camera(s) managed by the system. Background recordings will be stored as a discrete series of clips and will continue to operate in the event that communication between the Camera Server and the Database Server is lost. Once communication is restored, all relevant information will be updated to the Database Server.

For each camera, the user shall be able to configure the following (with descriptions as per User Activated and Event Activated recordings):

- Enable / disable background recording
- Duration of the recorded clip
- Frame rate for the recording
- Enable / disable archiving of the clip and the period after which to archive
- Retention period before the recording will be deleted
- Enable or disable audio recording (if available)
- Archive After period providing the period after which the recording will automatically be archived
- Delete After period providing the period after which the recording will automatically be deleted

Systems that require the configuration of multiple time periods to manage background recordings will not be accepted.

Continuous background recordings will not be dependent on network communications between the Camera Server and the Database Server. Once configured, these recordings will continue to operate in the event that this communication is lost.

4.6.6 VIDEO ANALYTICS RECORDING

The VMS system must be able to activate recordings automatically based on events generated by the real-time analysis of video from any camera on the system that has Video Analytics enabled. The real time analysis comprises several algorithms as follows:

- Video Motion Detection
- Object Tracking and Object Classification
- Intelligent Video Analytics based on Honeywell Intelligent Video Analytics or equivalent

4.6.6.1 Video Motion Detection

The VMS system must be able to support video motion detection algorithms, which can be executed by the video steamer or the Camera Server. The enabling of Video Motion Detection shall be either:

- On a continuous basis
- Scheduled for particular times, dates, days, months etc.

The Camera Server-based algorithms must be able to provide the following functionality:

- Detect or track objects
- Learn the scene

- Adapt to a changing outdoor environment
- Ignore environmental changes including rain, hail, wind, swaying trees and gradual light changes

The user shall be able to configure the following parameters for each camera:

- Detection Type: continuous or scheduled
- Actions to Perform When Motion is detected: when motion is detected, the following actions shall be performed automatically:

✓ Generate an alarm in the Security System, Building Control System or Industrial Control System of configurable priority (journal, low, medium, high)

✓ Start a recording, with the following configurable settings

  - Pre-Record Duration: The amount of pre-recorded video, allowing the Camera Server to capture video prior to the detection of motion, as well as after the detection of motion. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
  - Post Record Duration: Motion detection activated recordings shall terminate after this period.Shall be selectable from a list of values ranging between 0 seconds and 10 minutes or until motion has stopped. It shall be possible for the recording to continue until the motion detection algorithm considers motion finished.
  - Frame Rate: Video quality required for motion detection activated recording. Shall be selectable from the entire range of frame rates supported for the camera/streamer. For MPEG encoding (including H.264), support shall be provided to record only the Index frames, or a subset of the Index frames.
  - Retention Period: The Camera Server will retain the default period that motion deduction activated recordings before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.
  - Archive After period: The default period for which motion detection activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
  - Delete After period: The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per

camera but shall also be manually configurable on each individual recording after the recording has occurred.

- Send video to an operator station or alarm monitor: Automatically switch an operator station or alarm monitor to view the camera, which has motion detected.
- Trigger an output device on a related network camera or video encoder
- Motion Finished Time: The amount of time where no motion (inactivity) is detected before the previous motion is classified as completed. This shall be used for allowing recordings to continue until motion has finished.

  The VMS must provide a means of automatic and manual tuning of the Video Motion Detection for each camera. Incorporated within this tuning are the following:
  - Selection of the frame rate used for detection
  - Optimization for directions of movement
  - In any direction
  - Across the camera view
  - Towards and away from the camera
  - Sensitivity level to fine tune the motion detection algorithm
  - Specification of a minimum object size to allow noise filtering in the system to reduce false detections and alarms.

The VMS must also provide the ability to only detect motion in particular regions of the camera view. The ability to graphically select these regions using the mouse must be provided, with an unlimited number of regions permitted per camera. The regions of interest will be multi-vertical shapes with a minimum of six vertices to allow the region to be properly matched to the scene being detected. It shall be possible to add and remove vertices from the defined region of interest as needed.

Each region must be able to be individually tuned and have separate tuning parameters. This method of tuning must also provide a live tuning window whereby these settings and regions can be altered and tested prior to be being used. This live tuning window shall show the live video as well as regions of interest. During the time that motion is detected within a region, the border of the region shall change to a different color. In this way, tuning can be performed to achieve the desired performance. Text shall also be provided in the window to alert the user that motion has been detected.

4.6.6.2 Intelligent Video Analytics

The VMS must provide integration to an Intelligent Video Analytics system. The Intelligent Video Analytics system will be specified separately and will be based on Honeywell Intelligent Video Analytics or equivalent.

Video for analysis will be supplied to the Intelligent Video Analytics system algorithms by the Analytics Server(s) of the VMS. The Intelligent Video Analytics system will run on the VMS

Camera Servers and shall accept and process the video based on preconfigured conditions of interest.

Events from the Intelligent Video Analytics system will be passed back to the VMS for further action. It will be possible to automatically perform the following actions from the VMS based on events detected by the Intelligent Video Analytics system:

- Generate an alarm in the Security System, Building Control System or Industrial Control System of configurable priority(journal, low, medium, high)
- Start a recording, with the following configurable settings
    - Pre-Record Duration: The amount of pre-recorded video that will be associated with a device input/output. This shall allow the Camera Server to capture video prior to the alarm/event, as well as after the alarm/event. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
    - Record Duration: The period that the recording is active relating to the period of activity in the region of interest. Activated recordings will terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 10 minutes or the object is no longer in the region of interest.
    - Frame Rate: Video quality required for recordings triggered by events from the Intelligent Video Analytics system. Shall be selectable from the entire range of frame rates supported for the camera/streamer. For MPEG encoding (including H.264), support shall also be provided to record only the Index frames, or a subset of the Index frames.
    - Retention Period: The default period that recordings generated based on events from the Intelligent Video Analytics system will be retained by Camera Server before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.
    - Archive data: enable/disable archiving and set the period after which the recording will be automatically archived
    - Deletion data: Set the period after which the recording will be automatically deleted
    - Send video to an operation station or alarm monitor: Automatically switch an operator station or alarm monitor to view the camera which has motion detected
    - Trigger an output device on a related network camera or video encoder

It shall be possible to enable or disable the display of annotations associated with event detection delivered by the Video Content Analysis system on the VMS Operator Station

4.6.7 SNAP SHOT RECORDING

The VMS system must provide every operator with the ability to record the current frame of video. This snapshot of video shall be stored as a bitmap file. The file name shall be automatically generated by the VMS software and include the camera name, date and time of the recording (to millisecond precision). An audible sound shall be produced by the Client Computer, to ensure that the operator has feedback when the snapshot is taken.

4.6.8 RECORDED VIDEO

The VMs shall allow camera output to be recorded for the following conditions:

- Manually activated by a user viewing a live camera
- Activated bya Security System or Control System alarm or event
- Activated bt inputs or outputs on a streamer or IP Camera
- Continuous background recording
- Scheduled recording
- Specialized real-time video analysis Including:
  - Video Motion Detection
  - Intelligent Video Analytics
  - Camera Tamper events

User activated recording occurs when a user viewing live video chooses to record the currently viewed camera output by selecting the “Record” button.

Event activated recording is a process that allows a segment of video or a snapshot to be associated with a Security System, Building Control System or Industrial Control System alarm or event.

Input or output recording activation occurs when an input or output connected to an IP camera or streamer is activated and then subsequently triggers recording onone or more associated cameras.

Scheduled recording allows video to be recorded between start and stop times on defined days,

Real-time video analysis activated recording is a process that allows a segment of video or a snapshot to be recorded when a specific event is detected by a video analysis algorithms used by the VMS.

Recorded video is stored on the Camera Server. The Operator station shall be able to query the Database Server to locate relevant recorded video an to then replay that video at the Operator Station.

4.6.9 LIVE AND RECORDED AUDIO

The VMS shall provide the ability to have audio included with the video. Two types of audio support shall be provided:

- Single directional audio from the field (camera or streamer) locations to the VMS Camera Servers (and Operator Stations)
- Bi-directional audio between the field (camera or streamer) locations and the VMS Camera Servers (and Operator Stations)

4.6.9.1 Single Directional Audio

The VMs shall provide the following single directional audio support:

- Audio shall be recorded by the streamer using an attached microphone (or similar device)
- Audio shall be streamed along with the video from the camera (or streamer) locations to the VMs Camera Server(and Operator Stations) using the same network used for the video stream. This shall require no additional network cabling
- Audio shall be played at the Operator Stations using speaker connected to the Operator Station computer
- Live audio shall be played whenever the live video is displayed
- For scheduled and continuous (background) recordings, the audio shall be optionally disabled
- Audio shall be played when the recording containing audio is played. The audio shall be heard in the same synchronization it was recorded in.
- Whenever the audio is played with the video, a mute button and volume control shall be provided on the video player. It is unacceptable to use the Operating System’s volume controls for this purpose.
- Recordings containing audio shall be exported with the audio and video in the same synchronization it was recorded in.

4.6.10 PTZ- ACTIVATED RECORDING

The VMs shall support the ability to automatically commence recording on a PTZ camera when an operator takes control of the camera. The recording will commence when the user starts to control the camera and will stop after a predefined period.

PTZ-Activated recordings shall be identified by their own activation type to allow for easier searching and identification.

The user shall be able to configure the following parameters uniquely for each camera:

- Pre-Record Duration: The amount of pre-recorded video that will be associated with Intercom activated recording. This allows the Camera Server to capture video prior to the intercom request, as well as after the request. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.

- Frame Rate: Video quality required for intercom activated recording. It shall be possible to have different frame rates for intercom and event-activated recordings. Shall be selectable from the entire range of frame rates supported for the camera. For MPEG encoding (including H.264), support shall also be provided to record only the Index frames, or a subset of the Index frames.
- Record Duration: Intercom activated recordings shall terminate after this period.Shall be selectable from a list of values ranging between 0 seconds and 10 minutes.
- Retention Period: The default period that the Camera Server shall retain user-activated recordings before being deleted. The retention period of individual recordings shall be able to be changed on a per-recording basis. Shall be selectable from a list of values ranging between one hour and forever.
- Archive After period: The default period for which Intercom activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- Delete After period: The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting of all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

4.6.11 EDGE RECORDING

The VMs shall support the recording of video to storage on the IP Camera of video encoder. Video stored in this way will be accessible to VMS Operators for playback and export and to the system as a backup in the event of recording loss.

The VMS shall be ONVIF Profile G compliant and a certificate of conformance shall be listed on the ONVIF website as evidence.

Edge Recordings shall be configured directly in the device using the device webpage and recordings shall be stored on the Secure Digital (SD) Card installed in the device. Edge recordings shall be stored using H.264 encoding. Access to the edge recording shall be configurable on a per camera basis.

The VMS shall support the ability to backfill gaps in background recordings by using the recordings stored on the edge device. The VMS shall monitor for gaps in background recordings, determine whether a recording exists on the edge device for that period and then download the video data and store it as part of the background recording on the VMs storage subsystem. The backfill operation shall be automatic and not require any user interaction.

The VMS shall intelligently manage the backfill operation to ensure:

- Recordings that have been deleted from the VMs are not backfilled.
- The backfill operation shall be prioritized so that gaps in the most recent background recordings are filled first.
- The backfill of a long duration of missing recording is split into smaller time periods with a maximum duration 30 (thirty) minutes so as to prevent a single camera monopolizing the backfill operation over all other cameras.
- A sliding time window shall be maintained to ensure that the VMS only monitors for recording gaps that have occurred after the last backfill operation.
- The VMS shall provide a buffer of up to 6 (six) seconds of time synchronization difference between the VMS Servers and the camera. The backfill operation shall not be affected provided the camera time does not differ from the VMS server time by more than the defined buffer period.
- The VMS shall provide an alarm notification if the camera time starts to differ from the VMS Server time by more than the defined buffer period.
- All features in the video edge backfill operation shall be logged by the system for diagnostic purpose.

4.7 DEVICE CONFIGURATION REDUNDANCY

The VMS shall support the ability to configure more than a single instance of a camera. Each instance of the camera shall support unique configuration as allowed by the associated physical device.

It shall be possible to manage each instance of the camera by a separate Camera Server and record to a unique location to provide for redundant recording of video.

4.8 PRIVACY

Privacy of video data information is vital to protect the corporation using the VMS as well as those monitored by the system. The VMS shall provide the ability to further restrict access to recordings than the simple method of limiting operator access to specific cameras.

The VMS shall provide additional privacy control by requesting authorization for the review of recordings on cameras that have this feature enabled. The authorization will must be provided by a management level operator.

Authorization shall be provided by a second, unique user account to prevent any operator from authorizing themselves to review video recordings on affected cameras.

Operators authorizing the review of recordings shall be presented with a dialog box requesting their user name and password. They will also set the period for which the authorization is active, after which authorization will need to be obtained again to allow recording review.

Authorization success and failure shall be recorded the VMS audit log.

It shall be possible to set a grace period during which recordings can be immediately reviewed without authorization. Once this grace period has expired, operators will need to obtain authorization to review recordings on the affected camera(s).

It shall be possible to configure the need for authorized recording review on a per-camera basis. Systems enabling this feature as system-wide setting only will not be acceptable.

4.9 DIGITAL ZOOM AND IMAGE ENHANCEMENT

The VMS User Interface for Integrated Operator Station and Browser Clients shall support the following capability on both live and recorded video:

- The ability to digitally zoom into an area of the image
- The ability to enhance the image viewed by adjusting the levels of brightness, contrast, noise levels and sharpness.
  Digital zooming and Image Enhancement settings shall not be persistent and shall be reset on navigation away from the currently-viewed live or recorded scenes.
  Digital zooming and Image Enhancement settings shall only be applied to the image viewed by an operator making the changes on a specific operator workstation. The settings shall not affect other operator stations displaying the same video feed.

4.9.1 DIGITAL ZOOM

Digital zooming will be possible using all of the following methods:

- ‘Rubber-banding” using the mouse pointer, selects the area to zoom in to by clicking and dragging the pointer over the area of interest.
- Mouse Scroll Wheel point to the area of interest and rotate the mouse scroll wheel to zoom in and out.
- Using a zoom slider overlay or click on the “+” and “-“ digital zoom buttons on the digital zoom window

It shall be possible to return to the original scene by right- clicking anywhere in the video window or by clicking on a digital zoom overlay icon.

Once zoomed into an image, arrow will be overlaid onto the video window at the top, bottom, left and right of the image allowing for digital panning and tilting within the zoomed image.

The system shall provide the ability to switch between digital and analog zoom for cameras that support analog zoom for cameras that support analog zoom.

4.9.2 IMAGE ENHANCEMENT

It shall be possible to adjust the image brightness, contrast, noise levels and sharpness via slider bars accessed via buttons on the VMS video window.

4.10 SYSTEM AND USER AUDIT TRAIL

It is requirement that all user actions on the VMS Operator Station be recorded in a log file. User actions include:

- Interventions such as manual recording and configuration setting changes
- Cameras viewed
- Video replayed
- Video exported
- Cameras pan/tilt/zoomed and preset switching

This log must also contain a history of the status of the VMS system components. It shall list the status of all cameras, streamers, servers and other system components including when they were disabled or failed or a tamper occurred.

The log of user and system actions shall be available in text format and automatically included with any video recordings that are exported.

4.11 STORAGE

4.11.1 ONLINE STORAGE

The system shall hold a configurable amount of video in online storage. The amount of video stored on-line shall only be limited by the Camera Server’s disk capacity, the disk capacity of storage solutions attached to the Camera Server or the dedicated network storage allocated to the Camera Server.

For each Camera Server a limit on available storage space for on-line video shall be configurable.

The system shall support RAID 0+1, 1, 3,5 or 1+0 for video recordings (clips).

The VMS shall support storage on both NTFS and non-NTFS storage media. Systems that mandate the use of NTFS file systems for storage shall not be acceptable.

4.11.2 STORAGE & DISK ADMINISTRATION

The VMS shall provide a flexible means to configure storage behavior within the system administration displays. The system will provide an automated and configurable means to delete those remaining clips closest to their deletion criteria in order to increase available system storage. The disk space configuration will be separately configurable for each drive volume on each Camera Server.

Deletion will commence once the amount of available disk space drive volume on each Camera Server.

Deletions will commence once the amount of available disk space decreases to below a configurable limit. Alarms will be generated by the system to warn operators of this action. It shall be possible to configure the following parameters for this purpose:

- The Camera Server and volume being configured
- Threshold values for alarm generation (2 alarms low and very low)
- Enable or disable automatic deletion of clips based on available disk space
- The threshold value used to initiate the automatic deletion of clips
- Inclusion or exclusion of clips marked for archiving in automatic deletions
- Threshold value to stop recordings when available storage is critically low
- Threshold value to restart recordings when more disk space becomes available

The VMS shall provide a summary showing the available disk space, total disk space and number of recordings for directories used for this purpose on camera servers

4.11.3 AUTOMATIC ARCHIVING

The VMS shall provide the ability to automatically archive all records. It shall be possible to automatically archive any type of recording at a preconfigured period after the recording has complete.

It shall be possible to modify the automatic archive setting for each recording individually, as required.

In addition, the system shall also support manual archiving of video recordings.

4.11.4 OFF - LINE STORAGE

The Camera Sever shall be able to manage several off-line media devices for archiving and restoring video. The Camera Server must use an IT industry standard archiving method that is supported by the Microsoft operating systems specified within this document.

Offline storage shall be possible on non-NTFS storage devices. Systems that mandate the use of NFTS file systems for storage shall not be acceptable.

At least one ofthe following off-line devices shall be supported:

- Network storage solutions
- USB-connected storage devices
- DDVD-RW
- Magnetic tape media

If a user attempts to replay video stored in off-line media then the Camera Server will automatically restore and play the video if is accessible to an automated data retrieval system, or shall prompt the user the make the media containing the video available to the archive device.

4.12 INTEGRATED OPERATOR STATION

4.12.1 VIDEO INTEGRATION USE TASKS

The following system tasks shall be performed from the Operator Station

- View live video
- Adjust the PTZ position of a camera
- Live video is automatically displayed on a monitor when an event occurs
- Search through the stored video clips of a camera
- An operator records an incident
- Add a new camera to the system
- Delete a camera from the system
- Change the configuration settings for a camera
- Provide alarm/event activated recording from the integrated Security System, Building Control System of Industrial Control System
- Search for video clips from different cameras
- Define and export video evidence
- Create a sequence (camera tour)
- Conduct a sequence (camera tour)
- Create a multiple camera view
- View a multiple camera view
- View live video to a custom schematic
- Configure, schedule and tune Video Analytics
- Configure, schedule and tune camera tamper alarms
- Add new input or output devices on the streamers of IP cameras
- View the status of input or output devices on the streamers of IP cameras
- Command output devices on the streamers of IP cameras
- Change the configurations settings of input or output devices on the streamers of IP cameras
- View the audit log

- Digitally zoom into live or recorded video
- Adjust the brightness, contrast, noise levels and sharpness of live or recorded video
- Control the washer and wiper function on a supported camera
- Manually fail the Preferred Database Server to the Backup Database Server and vice versa
- Manually fail the Preferred Database Server to the configured Backup Camera Server of Camera Server Pool and vice versa

The following tasks shall also be performed from the Integrated Operator Station

- View the organization's Intranet from within the Operator Station window.

4.12.2 SECURITY, BUILDING CONTROL OR INDUSTRIAL CONTROL SYSTEM INTEGRATION USER TASKS

It shall be possible to perform the following tasks in the Security or Control System from the VMS Operator Station:

- Acknowledge an alarm
- Reset an acknowledged alarm
- Control a security or control system point
- Run a report containing proves control information
- Respond to security alarm
- View security and control system information on a process control schematic
- configure a point control schedule
- change an access level and download it to all affected access controllers
- view Access Controller details

All alarms and events from the VMS, Security and Control systems shall appear and be able to be managed from the same display on the Operator Station.

All alarms passed from the VMS to the Security, Building Control or Industrial Control Systems shall have configurable priorities.

The system shall support the display of live video within custom display screens of the Security system, Integrated Building Management System and Control System or Industrial Control System. The VMS system shall support the simultaneous display of dynamic data from the Security system, Integrated Building Management System and Control System or Industrial Control System and live or recorded video.

The system shall support the display of dynamic Intranet information on VMS displays

4.12.3 REPORTING

The VMS shall utilize the reporting infrastructure of the Security system, Integrated Building Management System and Control System or Industrial Control System to provide the following standard reports:

- System Bookmark Summary: A report detailing the operator bookmarks added to the system and including camera name, camera number, date, time and bookmark text
- Comprehensive Audit Report: A report displaying an audit trial of all VMS operator and system activities during a defined period
- System Activity Report: A report of actions and changes in the VMS during a defined period
- User configuration Report: A report providing details of user permissions including their security level and access rights to cameras, keyboards, mobile devices and facility locations
- User Activity Report: A report of all VMS user actions during a defined period
- Camera Configuration Report: A report detailing the camera configuration settings within the VMS
- Clip Summary Report: A report detailing the number and type of video clips recorded and which cameras were responsible for the recordings
- Storage Usage Report: A report detailing the available and consumed storage for specific Camera Servers in the VMS
- Video Analytics Event Report: A report detailing the video content analysis activity in the system during a defines period
- Controller Point Status Report: A report detailing the status of the VMS controller points within the Security system, Integrated Building Management System and Control System or Industrial Control System
- Process Point Status Report: A report providing the status of all VMS process points (cameras, control inputs and control outputs) within the Security system, Integrated Building Management System and Control System or Industrial Control System
- Camera Profile Configuration Report: A report providing the configuration of video stream profiles allocated to each camera

It shall not be acceptable to require that these reports be created using separate software products such as Crystal Reports of equivalent.

It shall be possible to define the start and end time for the reports listed above where applicable to a defined time.

4.13 IMAGE BLOCKING

The system shall provide the ability to limit he view of live and recorded video for specifically configured PTZ cameras to a specific group of users.

Images from these cameras will cease to be available to standard operators as soon as a user from the privileged group moves a camera away from its home preset position.

The ability to view live and recorded video from a camera that has had its imaged blocked in this manner shall be returned to normal once the privileged operator has stopped using the camera and the reservation period for that operator has lapsed.

4.14 NETWORK

The network Management Station shall perform the following functions:

- Provide a graphical display of the network topology
- Provide network traffic statistics for each LAN port
- Configuration of network equipment
- Support standard Management Information Bases (MIBs)

4.15 APPLICATION DEVELOPMENT INTERFACE

The VMS shall provide for the ability of custom developed applications to access and control the VMS system using a complete application development interface. These applications shall be able to be developed without the need to contact the VMS manufacturer. Complete documentation of this application development interface shall also be provided.

4.16 SYSTEM DIAGNOSTICS

The VMS shall provide diagnostic modules to assist with system health assessments and collection of diagnostic information.

The diagnostic applications shall provide a unified user interface for running test, recording system activity, collecting diagnostic information and viewing system log files.

It shall be possible to collect diagnostic information on all components of the VMS application including Database Servers, Camera Server, Clients and network activities.

4.17 SYSTEM MAINTENANCE

The VMS shall provide the ability to upgrade to future versions of the software without the loss of recorded video, except for the time taken to move a camera to Backup Camera Server.

Zero recording loss upgrades shall be accomplished by the combined use of Redundant Database Servers, Redundant Camera Servers and edge recording and backfill.

5. SERVICES

The vendor should be capable of providing supporting services as detailed in the following sections.

5.1 TRAINING

The vendor either at vendor's premises or on site shall provide standard training on all aspects of the system.

5.2 CONFIGURATION SERVICES

The vendor should be able to supply all necessary configuration services ig required including controller configuration, database configuration, etc.

5.3 INSTALLATION SERVICES

The vendor should be able to provide installation services for the system including validation services if necessary.

5.4 HARDWARE MAINTENANCE

The vendor should be able to provide hardware maintenance and spare parts support id required.

5.5 SOFTWARE ENHANCEMENT & SOFTWARE SUPPORT

The vendor should be able to provide a comprehensive software maintenance and enhancement program for on-going support of the system

9. COMMUNICATION NETWORK

Communication:

All communication between the host workstation, secondary workstation, and the CCTV shall via digital transmission through the SCCI Network and for construction site cameras-wireless network.

Data transmission:

The data transmission rate between the workstation and the servers shall be bi-directional using wireless network.

10. INTERFACES

The below listed interfaces are specified as an option & provisional scope, same to be finalized based on the site requirement and phases of the works.

Interface with ANPR and Arm Barrier (Provision)

Vehicle Security Check Point ANPR & Arm barrier(provision) need to be controlled through VMS; any contents need to be supplied by the Barrier Contractor

The sequence of operation and the interaction with the arm barriers, the automatic number plate recognition and its access control is to be proposed by the contractor for SCCI approval.

11. CAMERA LOCATION

Refer the layout Drawings

1. Basement Floor ………………………………………………………………………………… Page 64
2. Ground Floor …………………………………………………………………………………… Page 65
3. First Floor ……………………………………………………………………………………… Page 66
4. Roof Floor ……………………………………………………………………………………… Page 67

Note: Proposed camera locations are tentative for indication only: it will be finalized based on site works requirement & further design coordination

12. Rules and Regulations

12.1 SIRA Regulations

All items must be under SIRA law and regulations.

SIRA approved vendor is required to submit the proposal.

The vendors Engineers and Technician must be SIRA approved.

12.2 Sharjah Police Regulations

Implementing By-law and Decisions related to Sharjah police Law Concerning Security Service Providers and Users

13. ACCESS CONTROL SYSTEM

Access control system must be installed for CCTV control room door.

Note: All civil works related to install CCTV system must be included by the vendor.

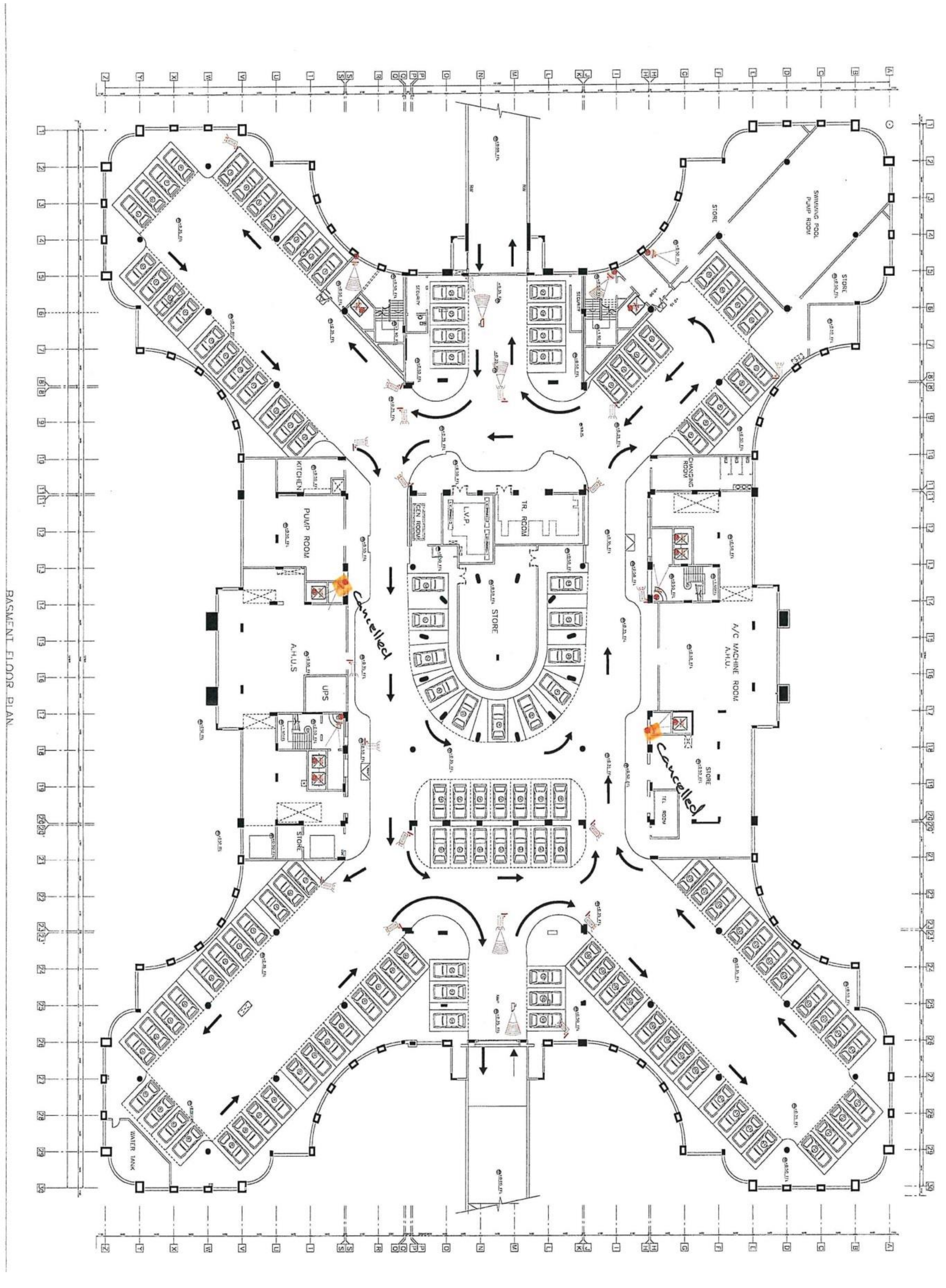
14.BOQ

SI NO		ITEM DESCRIPTION	BRAND	QUANTITY
CAMERAS AND ACCESSORIES				
1		2Megapixel Full HD Network IR Dome Camera Max. 2M (1920 x 1080) resolution , 2.8 ~ 12mm (4.3x) varifocal lens, 0.095Lux@F1.4 (Colour), 0Lux@F1.4 (B/W : IR LED on), 30fps@all resolutions (H.264), H.264, MJPEG dual codec, Multiple streaming, Motion detection, Tampering, DWDR, micro SD/SDHC memory slot, PoE, IR viewable length 15m, Hallway view support (Rotate 90˚/270˚) FIXED DOME CAMERA	SAMSUNG	80 NOS

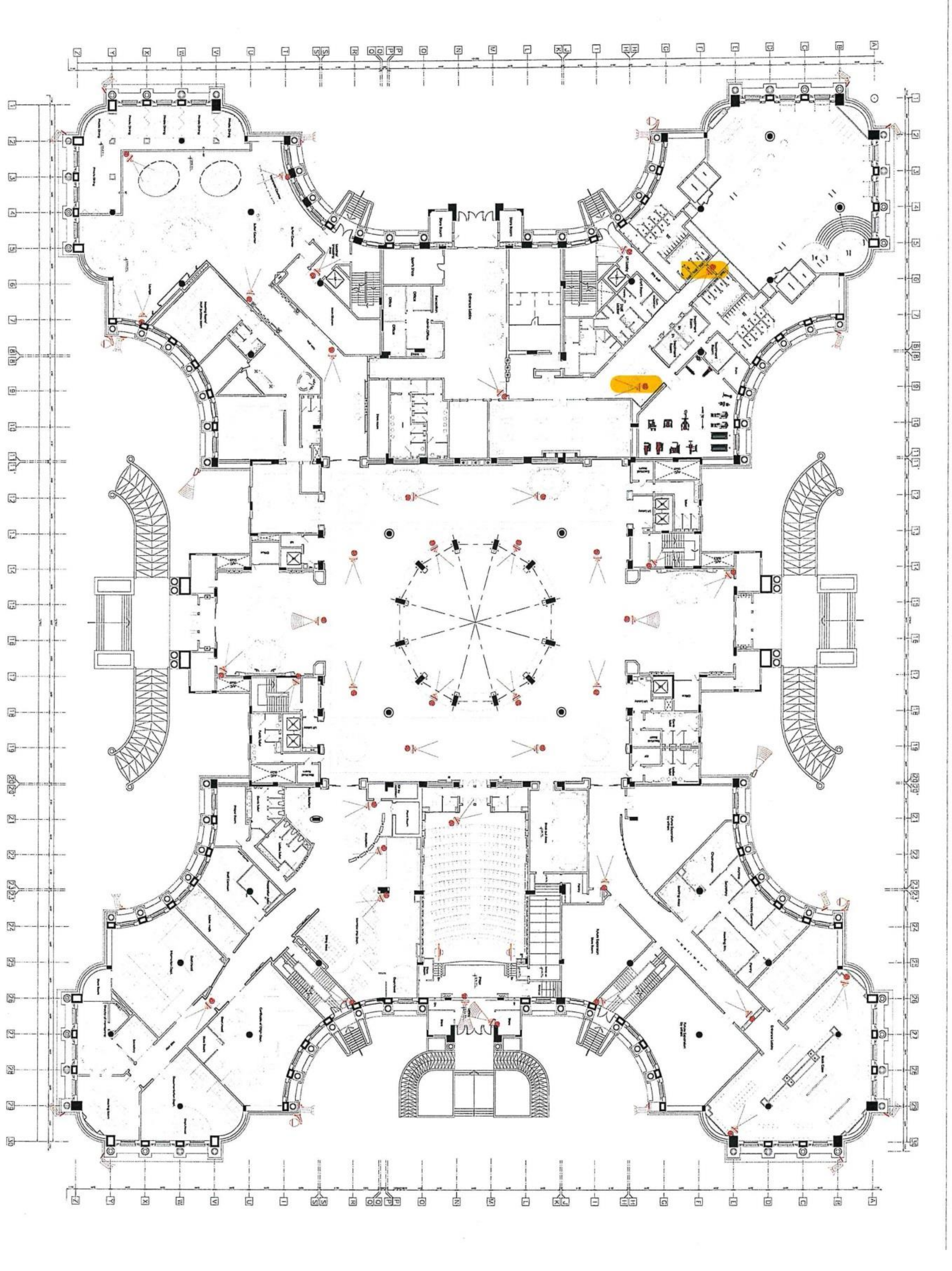
2		"2Megapixel Full HD Network Dome Camera Max 2M (1920 x 1080), Full HD(1080p) resolution , 60fps @ 1920 x 1080 , SSLE(Samsung Super Light Enhancer) 0.1Lux• Enhanced WDR (120dB)/ 30fps @2MP WDR , Built-in 3~ 8.5mm(2.8x) Varifocal lens , H.264 & MJPEG dual codec" WDR DOME CAMERA	SAMSUNG	6 NOS
3		"2Megapixel Full HD Weatherproof Network IR Camera Max. 2M (1920 x 1080) resolution , 2.8 ~ 12mm (4.3x) varifocal lens, 30fps@all resolutions (H.264) H.264, MJPEG dual codec, Multiple streaming , Motion detection, Tampering , micro SD/SDHC memory slot, PoE ,IR viewable length 20m, IP66, IK10" BOX CAMERA	SAMSUNG	40 NOS
4		"2Megapixel Full HD 32x Network PTZ Dome Camera 4.44 ~142.6mm (32x) optical zoom, 16x digital zoom , PoE+, SD/SDHC/SDXC memory slot, Bi-directional audio support , IP66 / NEMA4X / IK10 , Day & Night (ICR), WDR (120dB), Intelligent video analytics" PTZ Camera	SAMSUNG	5 NOS
5		• Max. 5M (2560 x 2048) resolution • Various viewing composition, 6 dewarping view mode • On board dewarping, Digital PTZ / Bi-directional audio • WDR (60dB), MD, AD • micro SD/SDHC/SDXC memory slot SAMSUNG FISH EYE CAMERA		
5		Wall Mount for PTZ Camera	SAMSUNG	5 NOS
RECORDING AND MONITORING				

6		32CH 4K Network Video Recorder-16TB Up to 32CH, Max. 12MP Camera supported , 256Mbps network camera recording , Support 4K video out on HDMI monitor , Support Dual monitor video out S,16TB,upport H.265, H.264, MJPEG compression , WiseStream support"	SAMSUNG	5 NOS
7		Video Management Software DSS4004 DAHUA and SAMSUNG SSM		1
ANPR SOLUTION FOR PARKING ENTRIES				
8		ANPR – TITAN HZM HD, Colour (or) CANDID (or) ARH	TITAN HZ (or) CANDID (or) ARH	4 NOS
9		TITAN HZ (or) CANDID (or) ARH	BASIC	1 NO
10		Server- TITAN HZ Basic w/19" Monitor (or) CANDID (or) ARH	TITAN HZ (or) CANDID (or) ARH	1 NO
11		Camera Configuration and Alignment		LS
12		Commissioning and Testing		LS
NETWORK ACCESSORIES				
13		24 Port POE Switch , Edge with SFP	ZYXel	6 NOS
14		48 Port POE Core Switch with SFP	ZYXel	1 NO

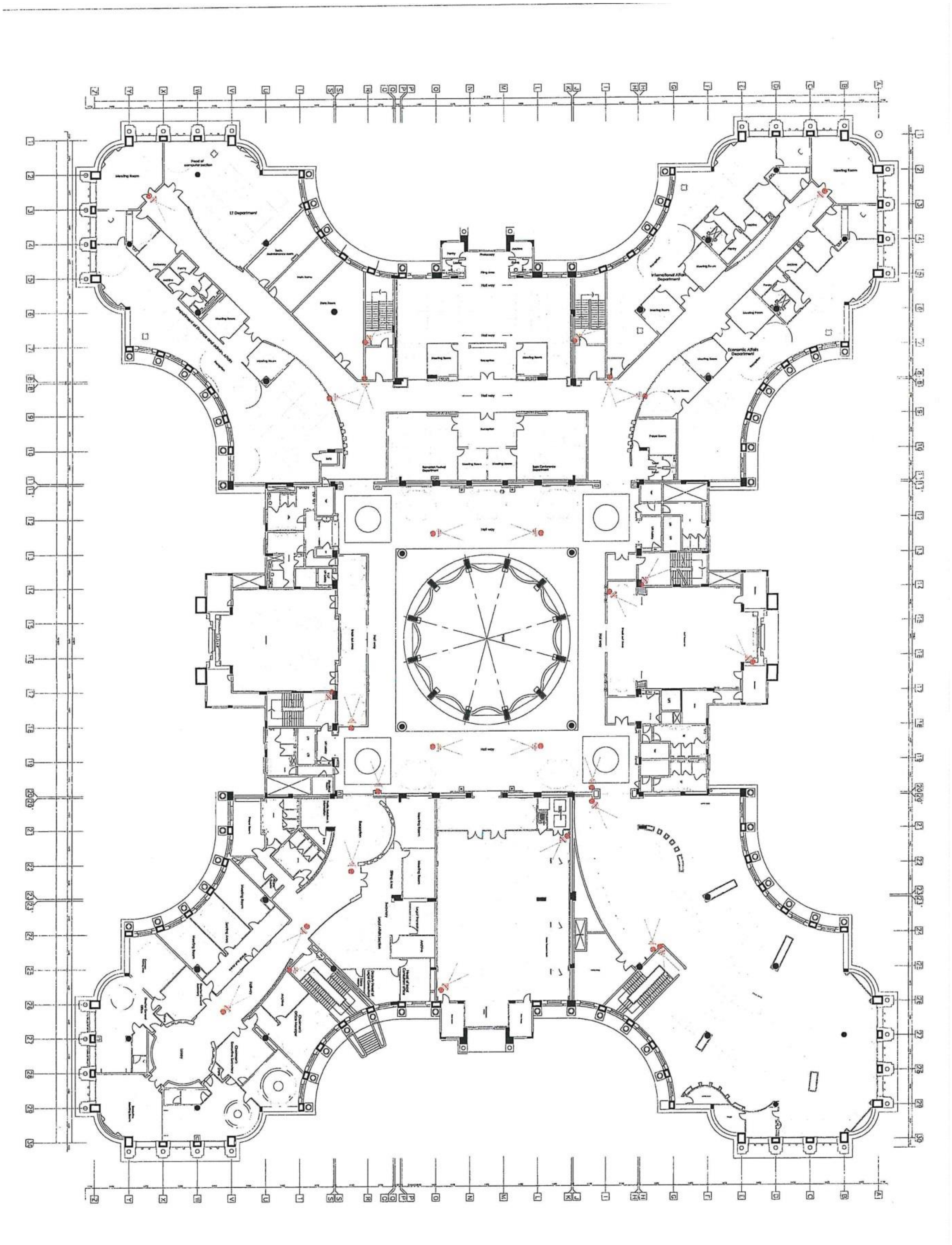
15		12U Cabinet for NVRs and Switches	Techlogiks	1 NO
16		Cat6 Cables and accessories and PVC Pipes and Trunk		LS
17		Cable laying , Conduit, and Cameras installation		LS
18		Testing and commissioning and Training		1 NO
MONITORING SYSTEM –VIDEO WALL SPLICING SCREEN ADVANCED SYSTEM				
19		DAHUA VIDEOWALL 55” SYSTEM SPLICING SCREEN(04 nos) 6 Channel HDMI Card(01) output cable-15M(06 nos) Video matrix(01) M70-4U-E（1.0.01.01.10947 (dahua)），Base for Display Unit Wooden Case for structure(01) Wooden Case for base(01) structure module(04) Splicing LCD tie rod(02) Splicing LCD Project(01) Accessory Kit		
20		21" Monitor for Playback/Spot		1 NO
ACCESS CONTROL SYSTEM- for the control room Door				
21		Zone Door, Zone Wing, HID RP10 BLE(reader),Magnetic Locks, U clamp, Break Glass		1 Each



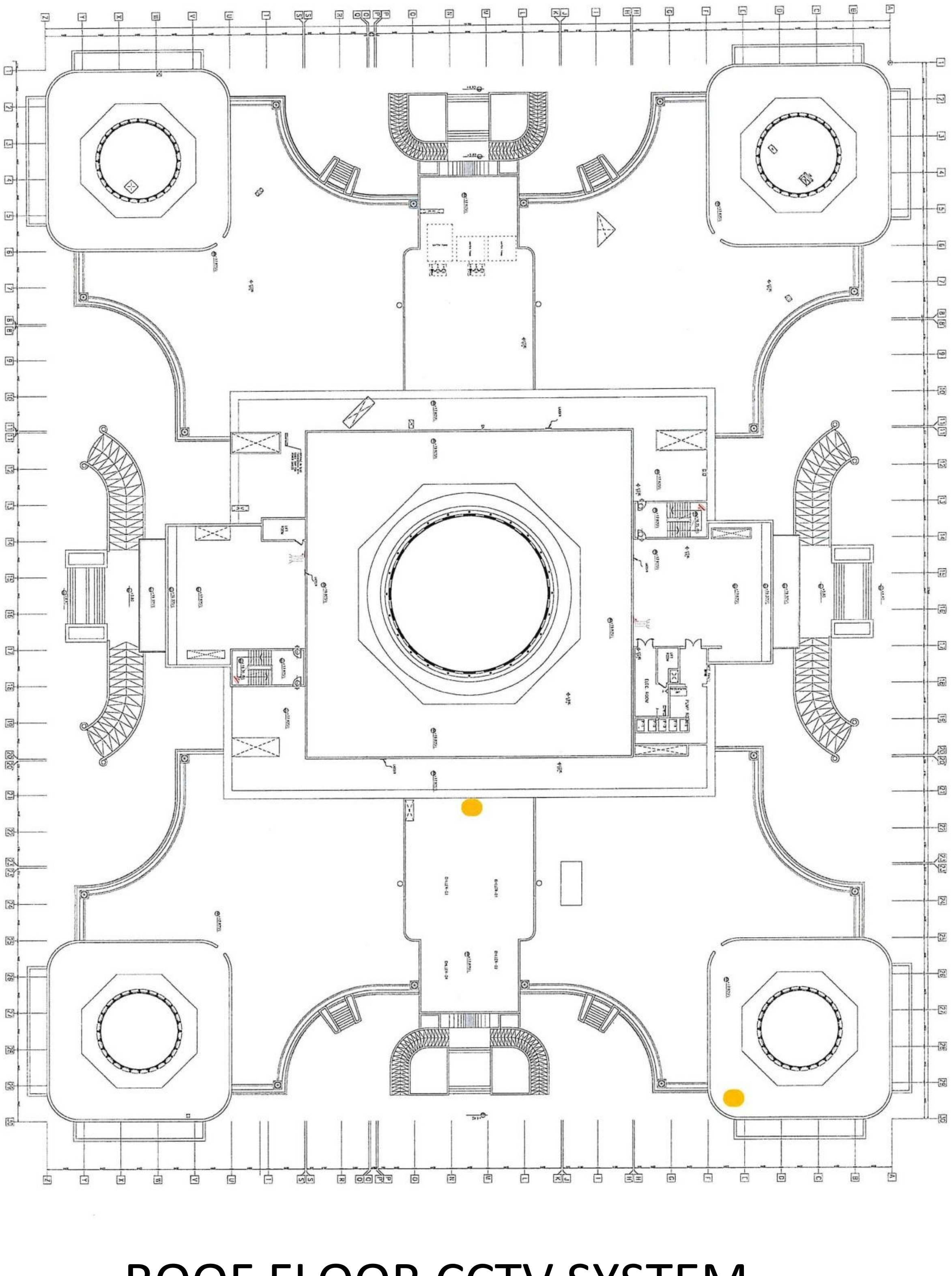
BASEMENT FLOOR



GROUND FLOOR



FIRST FLOOR CCTV SYSTEM



ROOF FLOOR CCTV SYSTEM