

October 29, 2021

(179 pages)

ADDENDUM NO. 4

BID CALL NO. T2021-173

CONSTRUCTION OF FIRE STATION 201 AT 25 RUTHERFORD ROAD SOUTH

This Addendum is part of the Bid Document.

Pertaining to Specifications and Drawings:

Refer to attached Consultant Addendum No. 3 (Total 178 pages).

All other terms & conditions remain unchanged.

If you have any questions, please do not hesitate to contact the undersigned.

Bidders are required to acknowledge all Addenda.

Santosh Mishra, CSCMP
Senior Buyer, Purchasing, Corporate Services
Ph: 905-874-3482
Email: santosh.mishra@brampton.ca

THE BID DOCUMENTS, CONDITIONS OF CONTRACT, DRAWINGS AND SPECIFICATIONS ARE HEREBY AMENDED, AS FOLLOWS:

Questions & Responses:

Question 1:

"Please provide the detail of Toe Wall (shown on Landscaping drawings)."

Response: Refer to civil drawings for detailing and OPSD references.

Question 2:

"For the proposed road extension from Rutherford to rear parking lot (shown on Landscaping drawings), please advise if it is heavy-duty."

Response: Refer to site plan drawing and legend on architectural drawing A101.

Question 4:

"Please advise if sidewalk & curb are monolithic."

Response: Sidewalk and curb are not monolithic. Refer to architectural and civil drawings.

Question 5:

"In the Hardware Schedule, it shows that that Power Supply, Proximity Reader, and Door Contact are by Security Contractor. Could you please provide the specs on what is required from a Manufacturer or model Number? There are also cameras noted on the drawings. But there is no information on model or spec."

Response: Refer to Electrical Addendum 03 issued herewith.

Question 5:

"There are three motorized dampers shown on drawing M302 related to compressor room 129. A sequence of operation has not been provided for these dampers. Please clarify if these dampers are to be controlled from the BAS and if so please provide a sequence of operation."

Response: Refer to Mechanical Addendum 03 issued herewith.

Amendment 1

TABLE OF CONTENTS – Section 00 01 10

- 1.1 Add section 07 46 16 – Aluminum Siding.

Amendment 2

ALUMINUM SIDING – Section 07 46 16

- 2.1 Add specification section 07 46 16 – Aluminum Siding issued herewith.

Amendment 3

ARCHITECTURAL DRAWINGS

- 3.1 Replace drawing A301 – North & South Exterior Elevations, with revision 10 dated October 29th, 2021 and issued herewith.
- 3.2 Replace drawing A302 – East & West Exterior Elevations, with revision 5 dated October 29th, 2021 and issued herewith.

Amendment 4

ELECTRICAL ADDENDUM

- 4.1 Refer to Electrical Addendum 03 dated October 29th, 2021 and issued herewith.

Amendment 5

MECHANICAL ADDENDUM

- 5.1 Refer to Mechanical Addendum 03 dated October 29th, 2021 and issued herewith.

Amendment 6

ARCHITECTURAL ADDENDUM 02

- 6.1 Revise response to Question 45 in Addendum 2 as follows:

Cabling, devices, headend equipment and installation for Intrusion detection, CCTV and access control are to be in the base bid by the security contractor. Refer to Quasar Electrical Addendum 03 issued herewith.

END OF ADDENDUM No. 3

1 General

1.1 **SECTION INCLUDES**

- .1 Design, labour, Products, equipment and services necessary for aluminum siding work in accordance with the Contract Documents.

1.2 **REFERENCES**

- .1 AAMA 2604 - Voluntary Specification, Performance requirements and Test Procedures for High Performing Organic Coatings on Aluminum Extrusions and Panels.
- .2 AAMA CW-10, Care and Handling of Architectural Aluminum from Shop to Site.
- .3 ASTM D4214, Standard Test Methods for Evaluating the Degree of Chalking of Exterior Paint Films
- .4 CGSB 93.5, Installation of Metal Residential Siding, Soffits and Fascia.
- .5 CAN/CSA-G40.20/G40.21M, General Requirements for Rolled or Welded Structural Quality Steel/Structural Quality Steels.
- .6 CSA S136, Cold Formed Steel Structural Members.
- .7 CSA W47.1, Fusion Welding Of Steel Company Certification.
- .8 CSA W47.2. Fusion Welding Of Steel Company Certification.
- .9 CSA W59-M, Welded Steel Construction (Metal Arc Welding).

1.3 **DESIGN REQUIREMENTS**

- .1 Design aluminum siding work in accordance with following Climatic Design Data for Brampton contained in the Ontario Building Code:
 - .1 Design temperature: January 1%, July 2 1/2%.
 - .2 Hourly wind pressures: 1 in 50 year occurrence.
- .2 Design aluminum siding system as a “dry joint system” and to withstand live, dead, lateral, wind, seismic, handling, transportation, and erection loads, imposed and other loads.
- .3 Design aluminum siding system to accommodate thermal movements of the components and structural movements to provide an installation free of oil canning, buckling, delamination, failure of joint seals, excessive stress on fasteners or any other detrimental effects.
- .4 Design aluminum siding system to prevent rattling and vibration of siding system, overstressing of fasteners and clips, and other detrimental effects on the system.

- .5 Siding removal: System design to allow removal of individual siding within system.
- .6 Design miscellaneous, additional structural framing members as required to complete aluminum siding system, where not indicated on Contract Drawings.
- .7 The attachment face of supporting the siding system must not deflect vertically more than 3 mm due to the dead load of the siding system.

1.4 **SUBMITTALS**

- .1 Product data:
 - .1 Submit copies of manufacturer's Product data in accordance with Section 01 30 00 indicating:
 - .1 Performance criteria, compliance with appropriate reference standard, characteristics, limitations.
 - .2 Product transportation, storage, handling and installation requirements.
 - .2 Shop drawings:
 - .1 Submit shop drawings in accordance with Section 01 30 00 indicating:
 - .1 Elevations, details, profiles, dimensions, thickness of materials, finishes, methods of joining, joint location, special joints, methods of anchoring, anchor and clip details, types of sealants and gaskets, waterproof connections to adjoining work, details of other pertinent components of the work, and compliance with design criteria and requirements of related work.
 - .2 Seismic anchors, supports and accessories for complete installation.
 - .3 Samples:
 - .1 Submit samples in accordance with Section 01 30 00:
 - .1 600 x 600 mm samples of siding system showing fully assembled components including aluminum siding, clip system and fasteners
Sample to be fabricated using exact colour and gauges specified.
 - .4 Closeout Submittals: Provide maintenance instructions for incorporation into Operation and Maintenance Manual, specified in Section 01 78 00.

1.5 **QUALITY ASSURANCE**

- .1 Retain a licensed Professional Engineer, registered in the Province of Ontario, to perform following services for prefinished siding work:
 - .1 Design of aluminum siding system.
 - .2 Design of anchors, supports and accessories to meet seismic requirements.
 - .3 Review, stamp, and sign shop drawings.
 - .4 Conduct shop and field inspections and prepare and submit inspection reports.

- .2 Perform work of this Section only by a Subcontractor of recognized standing who has adequate plant, equipment, and skilled workers to perform it expeditiously, and is known to have been responsible for satisfactory installations similar to that specified during a period of at least the immediate past ten years.
- .3 Execute steel welding to CSA W59-M by fabricators certified by the Canadian Welding Bureau to CSA W47.1.
- .4 Execute aluminum welding by fabricators certified by the Canadian Welding Bureau to CSA W47.2-M.
- .5 Execute finishing coatings and metal pre-treatments by applicators approved in writing by the manufacturer of the coatings and under the supervision of the manufacturer's qualified representative.
- .6 Mock-up:
 - .1 Fabricate, deliver, and erect a 3 m² mm high mock-up siding of aluminum siding system in location acceptable to Consultant.
 - .2 Demonstrate full siding fabrication and installation techniques, confirm stiffness/absence of deformation, finish, anchoring devices, air barrier sealing, joint detailing and sealing, and quality of workmanship.
 - .3 Mock-up may form part of final Work, if acceptable to Consultant. Remove and dispose of mock-ups which do not form part of Work.
- .7 Pre-Installation Meeting: Arrange meeting on Site to be attended by Consultant, Contractor, and siding manufacturer's representative to review installation procedures, interfaces with adjacent work, conditions under which work will be performed, inspect the surfaces to receive the vapour retarder, and installation procedures 48 hours in advance of installation.

1.6 **DELIVERY, STORAGE, AND HANDLING**

- .1 Handle aluminum work in accordance with AAMA CW-10. Protect aluminum surfaces with strippable coating. Do not use adhesive papers or sprayed coatings which bond when exposed to sunlight or weather. Do not remove before final cleaning of building.
- .2 Remove and replace all damaged and unsatisfactory materials which are deemed unsuitable for use at this Section's own expense.

1.7 **EXTENDED WARRANTY**

- .1 Submit an extended warranty for aluminum siding work in accordance with General Conditions, except that warranty period is extended to 3 years from date of Substantial Performance of the Work.
 - .1 Warrant against leaking, warping, twisting, joint, and finish failure.
 - .2 Coverage: Complete replacement including affected adjacent parts.

- .2 Manufacturer's Warranty: Provide siding manufacturer's written warranty naming Owner as beneficiary and covering failure of factory-applied exterior finish on prefinished metal sidings within the warranty period; warrant finish per ASTM D4214 for chalk not in excess of 8 NBS units and fade not in excess of 5 NBS units. Warranty period for finish: 15 years from date Work is certified as substantially performed.

2 Products

2.1 **ACCEPTABLE SIDING MANUFACTURER(S)**

- .1 Aluminum Batten: Vertical, 41 mm x 203.2 mm x 1.65 mm thick, extruded aluminum 6063-T5, 'Link & Lock Batten' by Longboard or approved alternative.

2.2 **MATERIALS**

- .1 All materials under work of this Section, including but not limited to, sealants, paints, and coatings are to have low VOC content limits.
- .2 Sheet aluminum: Aluminum Association 6061-T5 to ASTM B209.
- .3 Finish: Exposed to view: Powder coat finish complying to AAMA 2604, Colour: to match metal panel and soffit system in Section 07 42 41, unless indicated otherwise by Consultant. Concealed aluminum finish: Mill finish.
- .4 Structural shapes, plates, sag rods, and similar items: CAN/CSA-G40.20-G40.21-M, Grade 350W.
- .5 Fasteners: Concealed, ANSI B18.6.4, stainless steel Type 304.
- .6 Clips and Siding Reinforcement: Extruded aluminum or as recommended by siding manufacturer.
- .7 Provide all additional structural supports not shown on Drawings as required.
- .8 Seismic anchors, supports and accessories: In accordance with reviewed shop drawings.

2.3 **FABRICATION**

- .1 Fabricate facings and concealed support members in a manner which will provide an installation free of exposed fastenings, with sufficient support and allowance for thermal movement to prevent facing distortion. Take site measurements before proceeding with production.
- .2 Fabricate components of the system at factory, ready for field installation. Include full continuous joint reveals within system.

- 3. Fabricate facings flat, true, free of marks, without visible distortion and with edges straight and true. Make all planes true, and corners square and bend of minimum radius.
- .4 Provide proprietary aluminum extrusions to manufacturer's standard profiles for a complete installation. Extrusions shall be full length around siding perimeter for siding reinforcement and alignment. Intermittent clips are unacceptable.
- .5 Changes of plans, parallel or transverse to longitudinal axis shall be accomplished

3 Execution

3.1 EXAMINATION

- .1 Verify condition and dimensions of previously installed Work upon which this Section depends. Report defects to Consultant. Commencement of work of this Section means acceptance of existing conditions.
- .2 Verify that backup construction is aligned for proper installation of siding before commencing erection.
- .3 Protect metal surfaces in contact with concrete, masonry mortar, plaster or other cementitious surface and aluminum to steel surfaces with isolation coating.

3.2 INSTALLATION

- .1 Install aluminum fin in accordance with reviewed shop drawings and manufacturer's written instructions.
- .2 Maintain joints in exterior cladding true to line, tight fitting hairline joints.
- .3 Attach batten in a manner not restrict thermal movement.
- .4 Install batten system complete with all hardware and support anchoring as indicated in accordance with reviewed shop/erection drawings and manufacturer's printed instructions. Carefully co-ordinate work with other Sections.

3.3 REPAIR

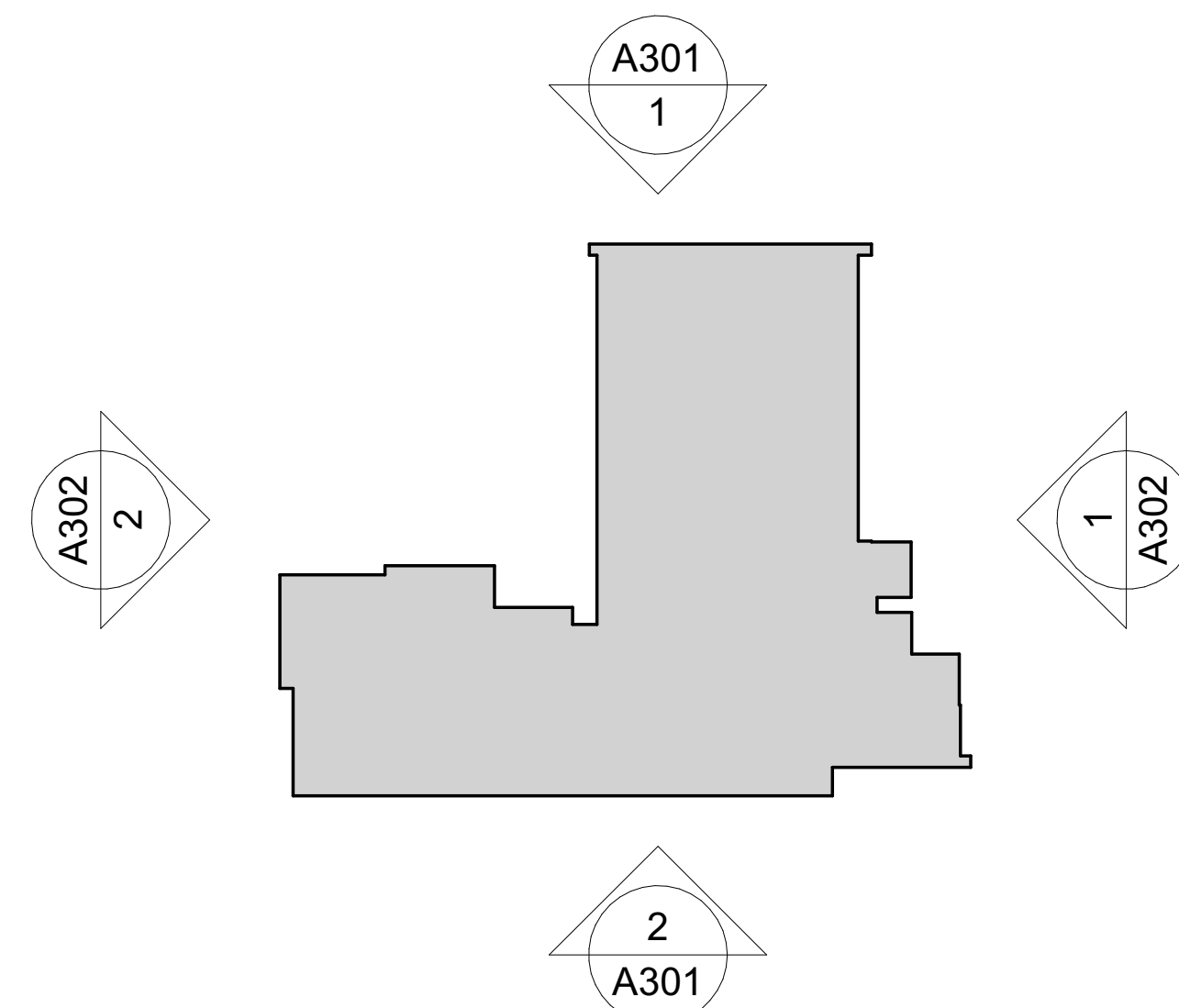
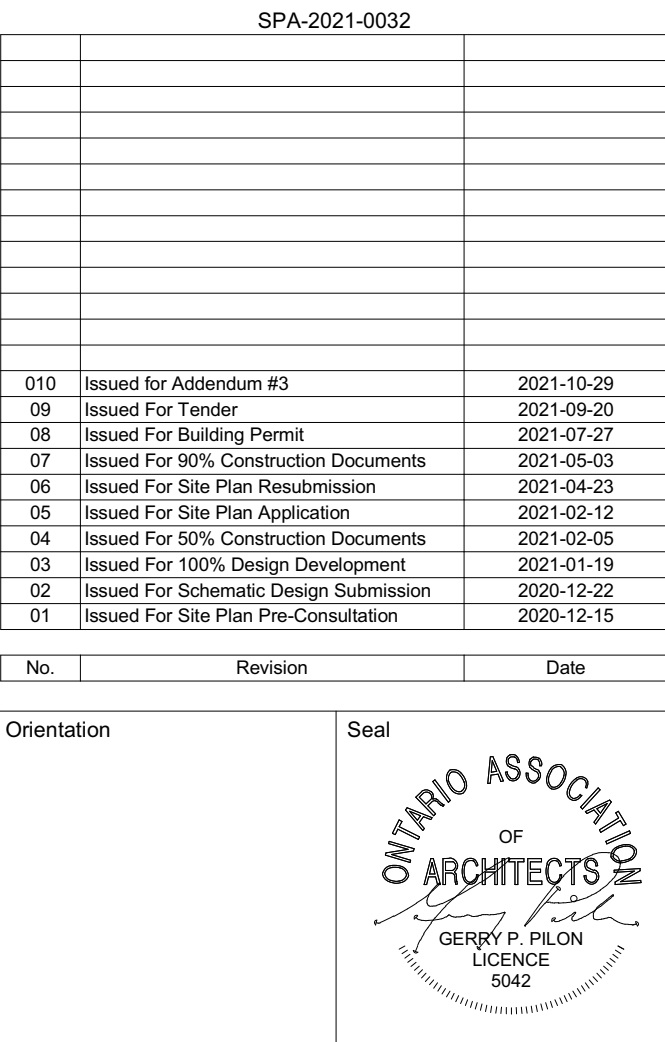
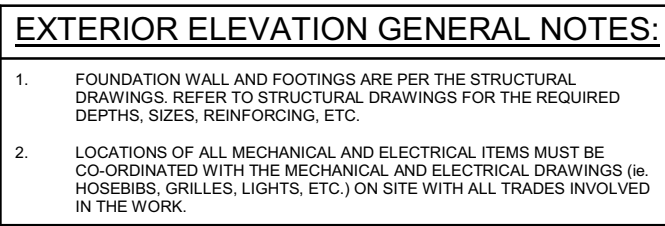
- .1 Remove damaged, dented, defaced, defectively finished, or tool marked components and replace with new, unless minor blemishes are approved by Consultant.
- .2 Only with approval of Consultant, refinish shop applied finishes in field with compatible materials to manufacturer's written instructions.

3.4 CLEANING

- .1 Remove all strippable protective film from the work as it is erected and prior to moving on to the next bay or grid.

- .2 Wash down exposed exterior surfaces using solution of mild non-acidic detergent in warm water, applied with soft clean wiping cloths.
- .3 As work progresses, remove excess sealant with recommended solvent and which will not affect metal, finished surfaces, or adjacent surfaces and materials.

END OF SECTION



All dimensions to be checked and verified on the job by the Contractor. Any discrepancies are to be reported to the Consultant prior to action. Only the latest approved drawings to be used for construction in conformance with all applicable codes, by-laws and regulations. All drawings remain the property of the Consultant.

© Copyright Reserved:
These drawings and all that is represented herein are the exclusive property of SALTER PILON Architecture Inc.
They may not be used or reproduced without written permission from SALTER PILON Architecture Inc.

salterpilon
architecture

151 Ferris Lane, Suite 400 Barrie, Ontario L4M 6C1
salterpilon.com t: 705.737.3530

Project Information

BFES Station 201

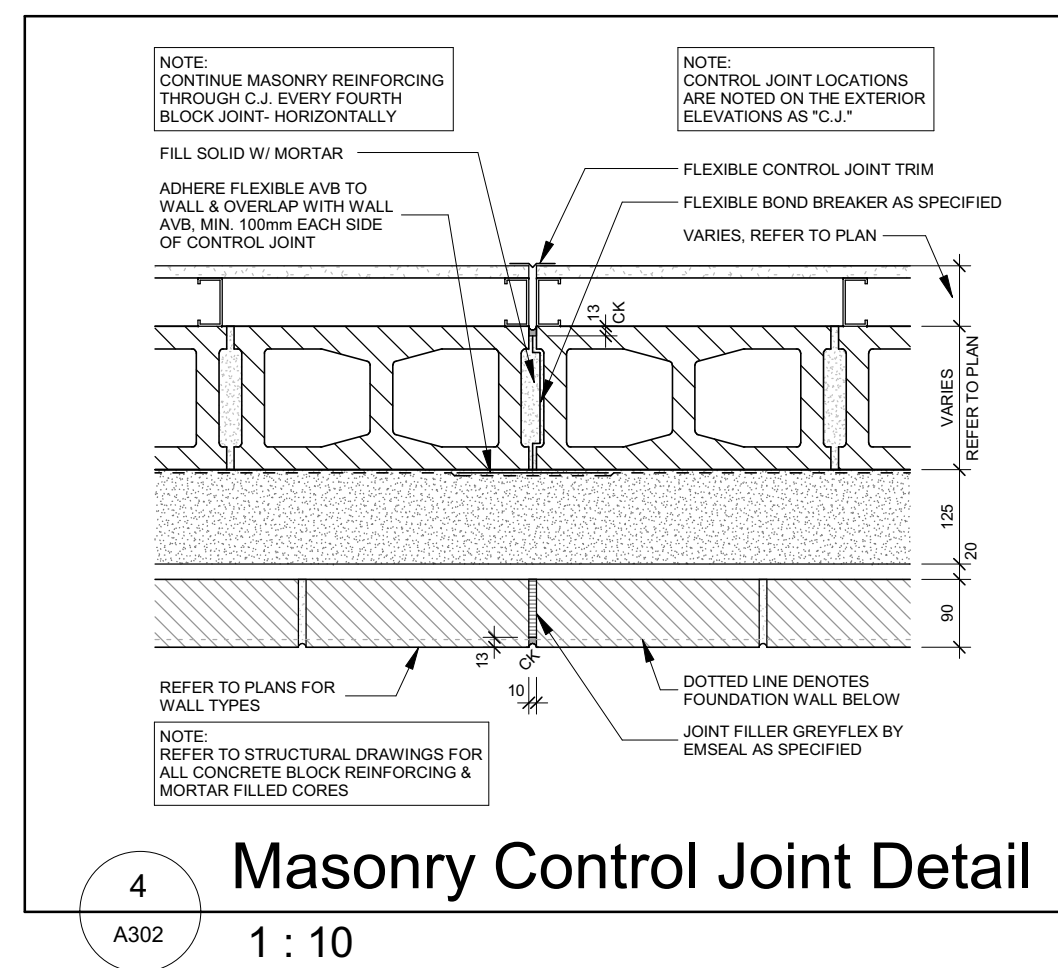
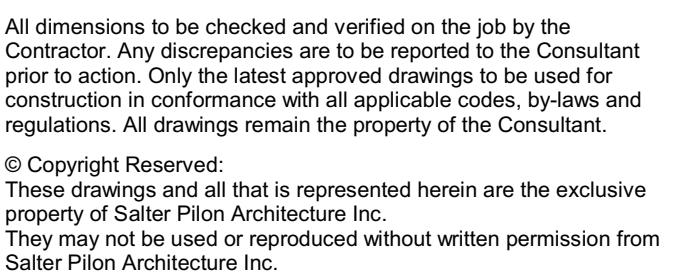
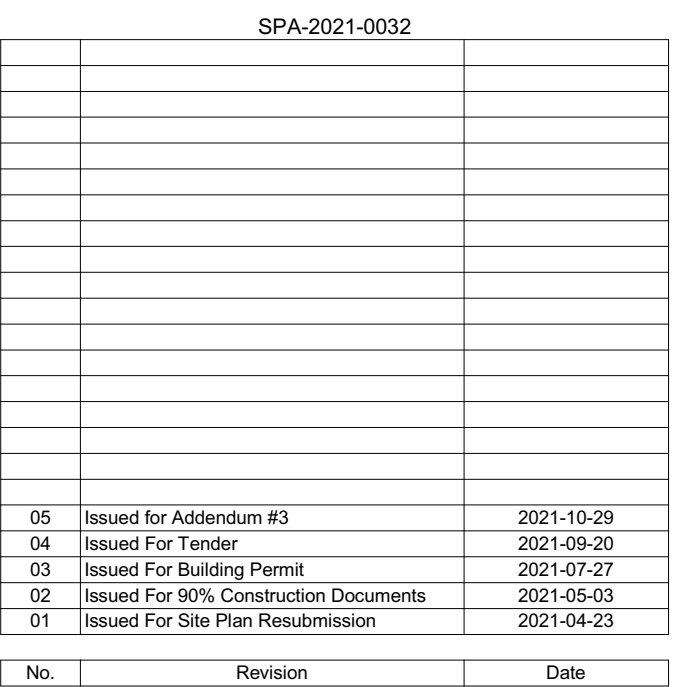
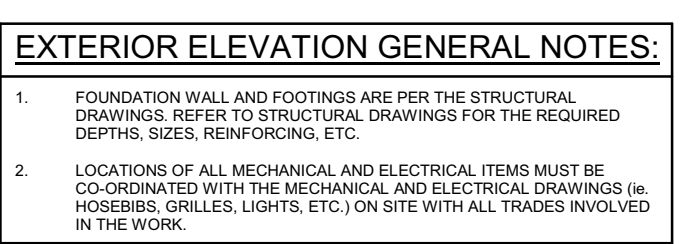
27 Rutherford Rd. S., Brampton, ON. L6W 3J3

For
City of Brampton Fire & Emergency Services

Drawing Title

North & South Exterior Elevations

Date	2021-10-29	Project No	Drawing No
Drawn by	BB, NL		
Scale	As indicated		



Project Name:	City of Brampton Fire Station 201	Date Issued:	October 29, 2021
Quasar Project #:	CM-21-083		
Client Project #:	20019		

Distribution

Salter Pilon Architecture	Ryan Stitt	rstitt@salterpilon.com
Salter Pilon Architecture	Brandon Bortoluzzi	bbortoluzzi@salterpilon.com
Salter Pilon Architecture	Nick Laurin	nlaurin@salterpilon.com

Addendum #: E03

Revision #: 0

This Addendum forms part of the Contract Specifications and Drawings, and modifies the Bidding Documents, with Amendments and Additions noted below. This Addendum shall be added to the front of the specifications as issued. Bidders shall acknowledge receipt of this Addendum in the space provided in the Bid Form and include in bid amount.

This addendum includes modifications to the drawings as summarized below. Unless otherwise noted, all drawings listed below are attached herewith.

Revisions to Specifications:

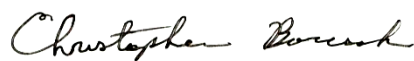
1. **Section 28 05 01 – Security Equipment**
 - a. Add new Section to the Specifications.
2. **City of Brampton - Security Equipment Design Standards and Equipment Specifications for New Construction and Facility Refreshment, Version 4.0 – June 2019.**
 - a. Add new document to specifications as referenced by Section 28 05 01.

Revisions to Drawings:

3. **Drawing E301 Level 1 Plan - Power & Systems**
 - a. In Lounge Area 119, delete two duplex receptacles and in lieu, add two split controlled receptacles on same circuits. Per note on legend, half of receptacle is automatically controlled. Integrate automatic control with lighting controls.

Questions and Answers:

1. **Drawing E301 Level 1 Plan - Power & Systems – Universal Washroom Equipment Acronyms**
 - a. Question: What do DRM, OL, and PL refer to?
 - b. Response:
 - i. DRM – “Door Release Module.” The intent of this push button is to allow for the fire station staff to restrict access to the universal washroom to only visitors that have been vetted by fire station staff.
 - ii. OL – “Occupied Light”
 - iii. PL – “Push to lock”
 - iv. Coordinate exact requirements with the door hardware schedule, and shop drawings for the door hardware and universal washroom emergency call system.

Quasar Consulting Group


Christopher Borcsok, P.Eng., LC, LEED AP

Senior Project Engineer

1 General

1.1 SECTION INCLUDES

- .1 Access Control, Video Surveillance, and other Security systems.

1.2 RELATED REQUIREMENTS

- .1 Section 27 05 28 – Interior Pathways for Communication System (Part of City of Brampton IT Performance Specification, Division 27, version 1.6, March 18, 2021.).
- .2 Section 27 05 28.61 - Pathways for Access Control and Intrusion Detection.
- .3 Section 27 05 28.63 - Pathways for Video Surveillance.

1.3 REFERENCES

- .1 City of Brampton – Security Equipment Design Standards and Equipment Specifications for New Construction and Facility Refreshment, Version 4.0 – June 2019.

2 Products

2.1 SECURITY SYSTEM COMPONENTS

- .1 Provide all components for a complete and fully functional system as described in the City of Brampton Security Equipment Design Standards and Equipment Specifications for New Construction and Facility Refreshment.
- .2 Requirements include, but are not limited to the following:
 - .1 Access Control Systems.
 - .2 Video Surveillance (CCTV).
 - .3 Power Sources for Electronic Safety and Security (UPS equipment).
 - .4 Servers, Workstations, and Storage for Electronic Safety and Security.
 - .5 Network Video Recorders.
 - .6 Communications equipment for Electronic Safety and Security, including racks.
 - .7 Network communications equipment.

3 Execution

3.1 INSTALLERS

- .1 Security Services Pre-Qualified Vendors
 - .1 Companies not included on this list will not be allowed to conduct work on City of Brampton projects.
- .2 Vendors List:
 - .1 M&R Security Inc.
Address: 46-16 Regan Road, Brampton, ON L7A 1C1
Contact: Amy Martinez
Email: amy@mnrsecurity.ca
Phone: (905) 216-6424
 - .2 V.S.I. Inc.
Address: 2650 Meadowvale Blvd, Unit #3, Mississauga, ON L5N 6M5
Contact: Len Todaro
Email: ltodator@vistasecurity.com
Phone: (905) 858-8211
 - .3 Vipond
Address: 6380 Vipond Road, Mississauga, ON L5T 1A1

Contact: Don Connor
Email: don.connor@vipond.ca
Phone: (416) 458-1990

- .4 SSN networks Inc.
Address: #24,1295Eglinton Avenue East, Mississauga, ON L4W 3E6
Contact: Ashish Kaushal
Email: ashish.kaushal@ssnnetworks.com
Phone: (647) 300-9194

- .5 Capital Fire and Security Inc.
Address: 52-665 Millway Avenue, Unit 52, Concord, ON L4K 3T8
Contact: Dino Abballe
Email: dino@capitalfireandsecurity.ca
Phone: (906) 660-0007

- .6 Colossus Security Inc.
Address: 55-3176 Ridgeway Drive, Mississauga, ON L5L 1K7
Contact: Jarrod Budd
Email: jbudd@colossussecurity.com
Phone: (888) 204-8833

3.2 INSTALLATION

- .1 Install security system components in accordance with attached City of Brampton document.

End of Section



City of Brampton

Security Equipment Design Standards and Equipment Specifications for New Construction and Facility Refreshment

Version 4.0 – June 2019

Document Owner: Mr. Scott Bagley
Supervisor, Security Systems
1-905-874-2356
Scott.bagley@brampton.ca

Revision History

Version	Date	Revised by	Description of Revisions
1.0	June 2011		Document Created
2.0	May 2012	Martin Dam beau	Inclusion of Transit recommendations, Introduction of Duress Event Stations (DES) and Key Control systems in Environmental Scenarios.
3.0	May 2014	Martin Dambeau	<ol style="list-style-type: none"> 1. Inclusion of Interior Space (A.x), Interior Space (B.x), Elevator (E.x), Outdoor Compound (C.x), Parking Garage (G.x), Parking Lot (L.x) and Service Garage (S.x) Environmental Scenario's 2. Performance Design Criteria (CCTV and Access Control). 3. Inclusion of CCTV Equipment Specifications, Access Control Specifications, DES Specifications and Intrusion Detection Specifications. 4. Inclusion of Asset Tracking Labeling Standards 5. Security Systems LAN IP Range Reservations
3.1	Sept 2014	Martin Dambeau	Updated IP Camera Models
3.2	Nov 2014	Martin Dambeau	Inclusion of Fibre Media Converters
3.3	April 2015	Martin Dambeau	Update Axis IP Camera Model
3.4	May 2015	Martin Dambeau	Update RBH Technologies Controller Specs (UNC-500)
3.5	May 2016	Martin Dambeau	<ol style="list-style-type: none"> 1. Update to Axis and Panasonic IP Camera Model 2. Update RBH UNC-500 Model number
4.0	May 2019	Scott Bagley	<ol style="list-style-type: none"> 1. Updated equipment specifications to Division 28 Master format. 2. Updated equipment installation typicals to new CAD format.

Table of Contents

Revision History	2
Section 1 - Introduction	5
Internal Design Consultation	5
Applicable Security Systems	5
Section 2 – Environmental Design Criteria Scenarios	7
Exterior Door Scenarios 1.x (common exterior doors mechanical and electrical rooms).....	7
Interior Door Scenarios 2.x (common interior doors including IT, mechanical and electrical rooms)	8
Interior High Security Door Scenarios 3.x (doors leading into high security areas including offices and workspace environments).....	9
Interior Space with Transaction Location Scenario A.x (common reception and service counter environments).....	9
Interior Space with High Security Scenario B.x (interior high value or confidential storage requirements and vault environments).....	10
Elevator Scenarios E.x	11
Outdoor Compound Scenario's C.x.....	12
Parking Garage Scenarios	13
Parking Lot (outdoor with open sky) Scenarios	13
Service Garage (Indoor Storage and Mechanical Garage) Scenarios	14
Section 3 – Equipment Specifications	15
Part 1 – General Requirements.....	15
1.1 General Conditions	15
1.2 Submittals.....	15
1.3 Quality Assurance.....	15
1.4 System Documentation	16
Part 2 – Products and Requirements	17
2.1 Supplies and System	17
2.2 Warranty.....	18
2.3 Access Control System General Requirements	18
2.4 Closed Circuit Television System General Requirements	19
2.5 Intrusion Detection System General Requirements	20
2.6 Intercom System General Requirements.....	21
2.7 Network Switches General Requirements	21
2.8 Network Media Extenders General Requirements	22
2.9 Backup Power Supplies General Requirements.....	22
2.10 Equipment Room Fittings General Requirements	22
2.11 Computers and Servers General Requirements.....	23
Section 3 Accepted Part Numbers by System Type	25
Section 4 – System Specifications	29
28 10 00 Access Control.....	30
28 23 00 Video Surveillance.....	56
VMS Applications	56
Network Video Recorders.....	66
Axis IP Cameras	83

1.03 video surveillance cameras	86
A. Fixed dome 3Mpxl network camera	86
B. Fixed indoor dome 1080p network camera	91
C. Fixed outdoor dome 1080p network camera	96
D. Fixed mini dome 720p network camera	102
E. 1080p PTZ network camera	107
F. PTZ dome 720p network camera	112
G. 1080p PTZ Dome network camera	118
H. Four Sensor Degree Camera with optional PTZ	123
Part 2 Execution	129
2.01 Installation	129
Panasonic IP Cameras – PTZ Dome Camera	130
Panasonic IP Cameras – Fixed Dome Camera	136
Panasonic IP Cameras – Panoramic Fixed Dome Camera	141
28 30 00 Security Detection, Alarm and Monitoring	145
28 50 00 Specialized Systems – Intercom Entry Systems	147
1.0 Technical Specifications – ES831/3A	147
2.0 Technical Specifications – EF 962H	148
3.0 Technical Specifications – GE 300 Server	149
4.0 Technical Specifications – GE 800 Server	150
26 33 00 Battery Equipment	152
27 11 00 Communications Equipment Room Fittings	154
2.0 Technical Specification – Full Height Rack	154
3.0 Technical Specification – Wall Mount Rack (10U)	155
4.0 Technical Specification – Wall Mount Rack (16U)	155
5.0 Technical Specification – Wall Mount Rack (22U)	156
27 20 00 Data Communications	157
3.0 Technical Specifications – 10 Port PoE Switch, SG250-10P	157
4.0 Technical Specifications – 24 Port PoE Switch @ 195W, SC250X-24P	158
5.0 Technical Specifications – 24 Port PoE Switch @ 375W, SC350X-24MP	160
27 22 00 Data Communications Hardware	162

Section 1 - Introduction

The use of Security Systems at City of Brampton facility's and corporate assets should be considered at the onset design of any new construction, and or facility or corporate asset refreshment. By capturing this component early in the overall scope of design, it will ensure that the technology required to enhance and provide City staff and its citizens with a safe work and municipal government environment, will fit seamlessly into the intended design and use of the asset.

The application, type of technology, and the specific equipment applied to all City facilities and assets, must adhere to the applicable legislated requirements and guidelines, as well as the City's overall design criteria and corporate wide capital investment.

Where the City is the owner of the facility, and third party tenants occupy portions of the building, Security Systems may be installed and administrated by the City, on behalf of the tenant. Tenants, who wish to install and administrate Security Systems within their own leased areas, may do so.

Where the City is a tenant in a facility, owned and operated by a third party, the Security Systems that are installed in public areas that are designed for City business practice (i.e. hallways, service counters) and that are installed and operated within the City's leased areas must be connected to the City's Security servers for administration and programming. Where the City is a tenant, and access to the facility is through common space, it is requested that Access Control measures are operated by the City's server to provide access for City staff to the leased areas. Areas that are not included as part of the leased space by the City, are not identified in this document. Security Systems required by the facility owner / operator shall be specified through their own requirements.

Internal Design Consultation

The Security Systems department of the City of Brampton is responsible for the internal consultation, review of proposed security system designs and layouts as provided by external consultants, and act as the City's representative to approve and accept systems that are incorporated in the design of any project. This internal consultation process ensures that the City's practices on the use and application of various security systems is adhered to and applied to the existing administration and operation of the devices.

Applicable Security Systems

The City of Brampton applies in various degrees, equipment and devices that are in some cases duplicate in function but are all operated by independent controllers. Where integration of equipment and devices are required in the design by the City, they are linked and operated through the system servers, not through device to device communications. Below are the basic foundations of the Security Systems that are deployed by the City of Brampton.

Closed Circuit Surveillance Systems (CCTV) – Include, but are not limited to;

- IP fixed and pan-tilt-zoom cameras, requiring network PoE/PoE+/hPoE/hPoE+ Cat 6a cabling connected to the City's IT or a local Security LAN infrastructure, that provide high quality video images to a network connected recording device.
- Managed networked recording device that is installed locally to the facility and accepts video images from IP and Analogue cameras and accepts hot swappable Hard Disk Drives and is capable of writing to DAS, NAS or SAN destinations.
- Uninterruptable Power Supply, for both the recording device(s) and the local Security LAN infrastructure, connected to base building power, and where available, circuits that are supported on the building's generator.

Access Control Systems (Card Access) – Include, but are not limited to,

- Intelligent readers with Proximity technology to read and provide door control at various control points, including man access doors, over-head doors, parking gates, and other means of barriers to control movement of people and assets.
- Access Control Controllers that are capable of receiving data from various devices including card readers, motion sensors, and to control output devices based on network server programming. Controllers must be capable of independent control when their network access to the main server is disconnected.
- Uninterruptable Power Supply, for Access Controllers, connected to base building generator circuits where available.

Intrusion Detection Systems (Burglary) – Include, but are not limited to,

- Input devices installed at strategic locations to monitor various environment changes, including motion, device tampering and damage.
- Controllers that receive information from input devices and provides communication out to a monitoring source for response.
- Uninterruptable Power Supply, for Intrusion Controllers, connected to base building generator circuits where available.

Duress Event Station Systems (also known as "Panic" alarms) – Include, but are not limited to,

- Communication devices (Stations) that include microphones, speakers, video displays, and IP enabled cameras installed at strategic locations to allow staff and public the opportunity to engage Security Services in a two way video and audio communication.
- Controllers that receive information from two way communication video and audio devices, and allows Security to engage devices in any combination, to engage communication.
- Duress event station systems are to be capable of integration to existing SIP telephony systems operated by COB IT
- Uninterruptable Power Supply, for Controllers, connected to base building generator circuits where available.

Key Control Systems – Include, but are not limited to,

- Networked electronic key cabinets that store and secure key rings.
- Controllers that control the distribution of keys based on configured programming and user access levels.
- Uninterruptable Power Supply, for Controllers, connected to base building generator circuits where available.

Section 2 – Environmental Design Criteria Scenarios

Exterior Door Scenarios 1.x (common exterior doors mechanical and electrical rooms)

Exterior Door Scenario 1.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors that lead directly into City staff only work environments that require regular access into the area.	Yes	Yes	Yes	No	N/A
Exterior Door Scenario 1.2	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors that lead directly into City staff only work environments that are intended for emergency egress only from the office area to the exterior.	Yes	No	Yes	No	N/A
Exterior Door Scenario 1.3	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors that lead directly into common public areas designated as a regular means of entry into the facility.	Yes	Yes	Yes	Yes	N/A
Exterior Door Scenario 1.4	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors that lead directly into common public areas designed as a means of emergency egress only from the interior to the exterior of the facility.	Yes	No	Yes	No	N/A
Exterior Door Scenario 1.5	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors that lead directly into Mechanical / Electrical / Building Operational environments that are used by the City.	Yes	Yes	Yes	No	N/A
Exterior Door Scenario 1.6	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors that lead directly into areas that are leased to tenants, where the City is the landlord.	Yes	No	Yes	No	N/A
Exterior Door Scenario 1.7	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors that lead directly into staff common areas used as kitchenettes, lunchrooms, etc.	Yes	Yes	Yes	Yes	N/A
Exterior Door Scenario 1.8	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors (including Over Head doors) that lead directly into City space that is used as a loading / shipping dock environment.	Yes	Yes	Yes	Yes	N/A

Exterior Door Scenario 1.9 (updated in V 2.0)	CCTV	Access	Intrusion	DES	Key Cont
Description: Exterior doors (including Over Head doors) that lead directly into City space that is used primarily as a shipping / receiving area / service counter environment.	Yes	Yes	Yes	Yes	N/A

Interior Door Scenarios 2.x (common interior doors including IT, mechanical and electrical rooms)

Interior Door Scenario 2.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into City staff only office style work environments that require regular access into the office area.	Yes	Yes	No	Yes	N/A

Interior Door Scenario 2.2	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into City staff only office work environments that are intended for egress only from the office area.	Yes	No	No	No	N/A

Interior Door Scenario 2.3	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into common public areas from other areas where the public may have general access.	Yes	No	No	Yes	N/A

Interior Door Scenario 2.4	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into common public areas from other areas where the public may have access, but is owned and operated by a third party (non-City)	Yes	Yes	Yes	No	N/A

Interior Door Scenario 2.5	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into boardroom type environments that are within areas already under access control.	No	No	No	No	N/A

Interior Door Scenario 2.6	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into boardroom type environments that are not within areas already under access control.	Yes	No	No	No	N/A

Interior Door Scenario 2.7	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into IT related rooms where access is shared with building operational trades and is used by the City.	Yes	Yes	No	Yes	N/A

Interior Door Scenario 2.8	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into Mechanical / Electrical / Building Operational environments that are used by the City.	Yes	Yes	No	Yes	N/A

Interior Door Scenario 2.9	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into staff common areas used as kitchenettes, lunchrooms, etc, that are within areas already under access control.	No	No	No	No	N/A

Interior Door Scenario 2.10	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into staff common areas used as kitchenettes, lunchrooms, etc, that are not within areas already under access control.	Yes	Yes	No	No	N/A

Interior Door Scenario 2.11	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into common IT related rooms where access is primarily used by IT authorized staff and higher level of control is required to protect the infrastructure within the room. (Does not include doors leading into a Main Server Room, see 3.x Scenarios)	Yes	Yes	No	Yes	N/A

Interior High Security Door Scenarios 3.x (doors leading into high security areas including offices and workspace environments)

Interior Door Scenario 3.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior doors that lead directly into a high security environment for the purpose of a Operational Control Room (i.e. Security Operational Control Room, Traffic Operations Centre).	Yes	Yes	No	Yes	Yes

Interior Space with Transaction Location Scenario A.x (common reception and service counter environments)

Interior Space Scenario A.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Service Counter where the primary transactions do not include values greater than \$50 (Including Transit environments)	Yes	Yes (after hours service counter separation)	Yes	Yes	N/A

Interior Space Scenario A.2	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Service Counter where the primary transactions include values greater than \$50, and where the public may also register disputes and or file legal actions. (Including Transit environments)	Yes	Yes (24 hour service counter separation)	Yes	Yes	N/A

Interior Space Scenario A.3	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Reception / Service desk where the public may request general information regarding the City and its services related to the facility and or asset. No financial transactions are conducted at this location. (Including Transit environments)	Yes	Yes (after hours service counter separation)	Yes	Yes	N/A

Interior Space Scenario A.4	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Reception / Service desk where the public may request access to a City Councilor or Official whose office is served by this control point. No financial transactions are conducted at this location.	Yes	Yes (after hours service counter separation)	No	Yes	N/A

Interior Space Scenario A.5 (updated in V 2.0)	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Reception / Service desk where transactions include pick-up / drop-off of small packages that are part of shipping / receiving processes. Financial transactions do not take place in this environment.	Yes	Yes (after hours service counter separation)	Yes	Yes	N/A

Interior Space with High Security Scenario B.x (interior high value or confidential storage requirements and vault environments)

Interior Space Scenario B.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Storage Room, where the items inside may contain personal staff property (i.e. Jackets, Boots) and general City stationary property.	No	No	No	No	N/A

Interior Space Scenario B.2	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Storage Room, where the items inside may contain general and confidential records regarding City business and operations.	No	Yes	No	Yes	N/A

Interior Space Scenario B.3	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Storage Room, where the items inside may contain staffing and high level confidential records regarding City business and operations.	Yes	Yes	No	Yes	N/A

Interior Space Scenario B.4	CCTV	Access	Intrusion	DES	Key Cont
Description: Interior Storage Room, where the items inside may contain valuables, currency, negotiable items and legal material. (i.e. Vault style room)	Yes	Yes	Yes	Yes	N/A

Elevator Scenarios E.x

Elevator Scenario E.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Elevator – where the primary operation is by public and staff who require access to various open and secured floors.	Yes	Yes	No	Yes	N/A

Elevator Scenario E.2	CCTV	Access	Intrusion	DES	Key Cont
Description: Elevator – where the primary operation is by staff only who require access to various open and secured floors.	Yes	Yes	No	Yes	N/A

Elevator Scenario E.3	CCTV	Access	Intrusion	DES	Key Cont
Description: Elevator – where the primary operation is by contractors and operational maintenance staff who require access to various open and secured floors. (typical “service elevator”)	Yes	Yes	No	Yes	N/A

Elevator Scenario E.4	CCTV	Access	Intrusion	DES	Key Cont
Description: Elevator – where the primary operation is by public and staff who require access to various open floors that are not control (typical in a parking garage)	Yes	No	No	Yes	N/A

Outdoor Compound Scenario's C.x

Outdoor Compound Scenario C.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Compound where there is only COB access and has 100% perimeter fencing with one or more vehicle access points and one or more pedestrian access points. <i>The compound stores vehicles and other high value equipment assets. (seasonal and year round)</i>	Yes	Yes	Possible	Yes	N/A

Outdoor Compound Scenario C.2	CCTV	Access	Intrusion	DES	Key Cont
Description: Compound where there is only COB access and has 100 % perimeter fencing with one or more vehicle access points and one or more pedestrian access points. <i>The compound typically does not store vehicles and other high value equipment assets, but does store operational material such as stones, soil and other consumable items. (seasonal and year round)</i>	Yes	Yes	No	Yes	N/A

Outdoor Compound Scenario C.3	CCTV	Access	Intrusion	DES	Key Cont
Description: Compound where there is COB and or shared (3 rd party) access and has 100% perimeter fencing with one or more vehicle access points and one or more pedestrian access points. The primary use of this area is typically for vehicle traffic only during operational hours. <i>The compound typically does not store vehicles, high value assets and other operational materials. (seasonal and year round)</i>	Yes	Yes	No	No	N/A

Outdoor Compound Scenario C.4	CCTV	Access	Intrusion	DES	Key Cont
Description: Compound where there is COB and shared (3 rd party) access and has 100% perimeter fencing with one or more vehicle access points and one or more pedestrian access points. <i>The compound stores vehicles and other high value equipment assets. (seasonal and year round)</i>	Yes	Yes	No	No	N/A

Outdoor Compound Scenario C.5	CCTV	Access	Intrusion	DES	Key Cont
Description: Compound where there is COB and shared (3 rd party) access and has 100 % perimeter fencing with one or more vehicle access points and one or more pedestrian access points. <i>The compound typically does not store vehicles and other high value equipment assets, but does store operational material such as stones, soil and other consumable items. (seasonal and year round)</i>	Yes	Yes	No	No	N/A

Parking Garage Scenarios

Parking Garage Scenario G.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Common Public and COB staff parking access areas including parking stalls and roadways.	Yes	No	No	Yes	N/A
Parking Garage Scenario G.2	CCTV	Access	Intrusion	DES	Key Cont
Description: Common Public and COB staff Elevator Lobby areas leading to the exterior and or common parking stalls and roadways.	Yes	No	No	Yes	N/A
Parking Garage Scenario G.3	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only parking access areas including parking stalls and roadways where the public may have pedestrian access.	Yes	No	No	Yes	N/A
Parking Garage Scenario G.4	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only parking access areas including parking stalls and roadways where the public does not have normal access.	Yes	Yes	No	Yes	N/A
Parking Garage Scenario G.5	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only access areas related to Parking Garage Operations that would not be covered under 1.x, 2.x, 3.x, A.x or B.x scenarios.	Yes	Yes	Possible	Yes	N/A

Parking Lot (outdoor with open sky) Scenarios

Parking Lot Scenario L.1	CCTV	Access	Intrusion	DES	Key Cont
Description: Common Public and COB staff parking access areas including parking spots and roadways.	Yes	No	No	No	N/A
Parking Lot Scenario L.2	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only parking access areas including parking spots and roadways where the public may have pedestrian access.	Yes	No	No	No	N/A
Parking Lot Scenario L.3	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only parking access areas including parking stalls and roadways where the public does not have normal access.	Yes	Yes	No	Yes	N/A
Parking Lot Scenario L.5	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only access areas related to Parking Lot Operations that would not be covered under 1.x, 2.x, 3.x, A.x or B.x scenarios.	Yes	Yes	Possible	Yes	N/A

Service Garage (Indoor Storage and Mechanical Garage) Scenarios

Service Garage Scenario S.1	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only areas where the storage of vehicles and high value equipment assets.	Yes	Yes	Possible	Yes	N/A

Service Garage Scenario S.2	CCTV	Access	Intrusion	DES	Key Cont
Description: COB staff only areas where the mechanical maintenance and cleaning of COB vehicles take place.	Yes	Yes	Possible	Yes	N/A

Section 3 – Equipment Specifications

Part 1 – General Requirements

1.1 General Conditions

- .1 The Supervisor, Security Systems with the City of Brampton, will be the designated contact for the owner / client.
- .2 All submitted system designs and proposals are to include all required client and server software licenses to ensure full system functionality and access for Security Systems staff.
- .3 The vendor will provide evidence of their status as a certified vendor as well as current technical certifications for installation staff for all March Networks, RBH, and Commend products being installed at any City of Brampton location. Acceptable evidence is a letter indicating that the integrator is a vendor in good standing with the manufacturer along with copies of all technician certifications, or a list of certified technicians, with the level of certification achieved from the manufacturer.

1.2 Submittals

- .1 For new construction projects, the proposal submitted by the security equipment vendor shall include the following:
 - .1 Current and future state system architecture drawings.
 - .2 System riser drawing indicating cabling pathways.
 - .3 A functional narrative describing the operation of the system as a whole, as well as at the individual component level; including any 3rd party system integrations and data or manual system input dependencies.
 - .4 Logical network architecture drawing including a schedule of all required ports and protocols, and data flows between system elements and third party applications i.e. Active Directory, Mail Services, 3rd party integrations, etc.
 - .5 Equipment schedules for all hardware that clearly identifies each installed component by make and model number.
 - .6 Data sheets indicating the functional specifications of each unique device are to be submitted as part of the proposal submittal.
 - .7 Letters from ACMS, CCTV, Intrusion, and Intercom manufacturers indicating the company's current status as a certified vendor and installer of the products.

1.3 Quality Assurance

- .1 All components shall be CSA and/or ULC approved listed and labelled.
- .2 The bidder shall be a certified reseller in good standing of the security systems and components selected and will employ staff with current training certifications said systems and components.
- .3 The City of Brampton requires that all low voltage cabling shall the minimum specifications detailed below:

- .1 Utilize cabling, patch panels, connectors, etc. from the following brands: Corning, Belden, Commscope, Provo, and specialty brands as required and approved by COB Security Systems Staff.
- .2 Provide cabling, patch panels, connectors that are from the same manufacturer to ensure end to end compatibility and compliance with cabling manufacturer extended warranty programs.

1.4 System Documentation

- .1 Upon final acceptance of the installed system or components by the City of Brampton Supervisor, Security Services, the integrator shall provide a set of system documentation that includes:
 - .1 All of the items listed in 1.2.1.1 through 1.2.1.6 for the system as installed and accepted by the client.
 - .2 Documentation of each installed component including:
 - .1 Make
 - .2 Model
 - .3 Serial Number
 - .4 COB Asset Label # where applicable
 - .5 Installation location
 - .6 Cable source termination location and cable ID
 - .7 Device specific configuration information i.e. O/S, CPU, RAM, HDD for NVRs, servers, and workstations, IP addressing information for network connected devices, camera installation parameters (height, lense, housing, description of FOV, live view and recording stream settings), etc. All device network configuration information will be provided to the security vendor by City of Brampton Security Services staff.
 - .3 Configuration backups of all system devices capable of exporting a backup file in electronic format.

Part 2 – Products and Requirements

2.1 Supplies and System

- .1 The door access control system specified herein is the product of RBH Access Technologies Inc. ([http:// http://www.rbh-access.com/](http://http://www.rbh-access.com/)) and is known as “Axiom”. No other equivalent access control systems will be considered.
- .2 The card readers specified herein are the product of HID Global (<https://hidglobal.com>). No other equivalent card readers will be considered.
- .3 The enterprise video management system specified herein is the product of March Networks Corporation (<https://marchnetworks.com>) and is known as “Command”. No other equivalent video management systems will be considered.
- .4 The network connected digital video recording devices specified herein are the product of March Networks Corporation (<https://marchnetworks.com>). No other equivalent video management systems will be considered.
- .5 The IP and analog cameras specified herein are the products of Axis Communications (<https://axiscommunications.com>) and Panasonic (<https://na.panasonic.com/ca/safety-security/video-surveillance/>). No other equivalent IP or analog cameras will be considered.
- .6 The intrusion detection system specified herein is the product of Digital Security Controls by Tyco (<https://www.dsc.com/>). No other equivalent intrusion detection system will be considered.
- .7 The intercom and paging systems specified herein are the product of Commend International (<https://www.commendusa.com/>). No other equivalent intercom and paging systems will be considered.
- .8 The Layer 2 and Layer 3 network switching solutions specified herein are the product of Cisco Systems Inc. (https://www.cisco.com/c/en_ca/index.html). No other equivalent networking products will be considered.
- .9 The network media extension devices specified herein are the product of Black Box Corporation (<https://www.blackbox.com/en-ca>). No other equivalent network media extension technology will be considered.
- .10 The battery backup systems specified herein are the product of APC by Schneider (<https://www.apc.com/ca/en/>). No other equivalent battery backup systems will be considered.
- .11 The equipment racking systems specified herein are the product of Middle Atlantic Products (<https://www.middleatlantic.com/>). No other equivalent battery backup systems will be considered.

- .12 The computers and server equipment specified herein are the product of Dell or HP (<https://www.dell.com> or <https://www.hp.com>). No other computer or server equipment will be considered.

2.2 Warranty

- .1 The System Supplier shall provide a warranty on the system which shall include all necessary labor and equipment to maintain the system(s) in full operation for a period of two years from the date of acceptance.
- .2 System Supplier shall provide, free of charge, product firmware/software upgrades throughout the warranty period for any product feature enhancements.

2.3 Access Control System General Requirements

- .1 Supply and install a complete and operational door access control system consisting of control panels, door contacts, RTE motion sensors, electric strikes, magnetic locks, proximity card readers, interface accessories, interface hardware, power and signal cables, conduits, wireways, power supplies, necessary software, programming and commissioning.
- .2 Systems shall be as shown on the drawings and herein specified.
- .3 All cabling for the door access control system shall be run in conduit, unless otherwise indicated on the drawings or advised by City of Brampton Corporate Security Service staff and shall be concealed in finished areas. All cabling to meet City of Brampton standards stated in section 1.3.3.
- .4 The normal power supply to the door access system shall be 120 Volts 60 HZ taken from the building service at the closest panel. Provide new breaker in existing panel to match existing breakers if required. Power from the building service shall be dedicated to the door access system and not shared by any other system.
- .5 Ensure equipment manufacturer provides all information regarding wiring, conduit runs and component requirements before tendering. Owner will not be responsible for added costs and charges due to additional manufacturer's requirements.
- .6 Provide network switch for communication and camera power supply over PoE/PoE+/hPoE/hPoE+ with capacity based on the noted project equipment matrix and design layouts sized to suit the total connected camera load plus 25% PoE capacity and 25% port capacity to allow for future expansion.
- .7 The vendor shall all engage in all commercially reasonable efforts to supply and install edge devices that have undergone the following configuration hardening as a minimum security standard:

- .1 Disabling any non-encrypted communication protocols i.e. FTP via Port 21, SMTP, POP server access, web access via port 80, etc.
- .2 Updating default administrator passwords
- .3 Disabling any device discovery protocols and SNMP
- .4 Enabling secure communications protocols i.e. HTTPS via SSL, SecureFTP via SSH, etc.

2.4 Closed Circuit Television System General Requirements

- .1 Supply and install a complete and operable closed circuit television (CCTV) system consisting of visible and near visible spectrum cameras complete with lenses, housings and mounting hardware as specified in the drawings CCTV schedule, IP and hybrid network video recorder(s), UPS, alarm interface accessories (where specified), interface hardware, power and signal cables, network connections, conduit where required, wireways, console rack, network switches for communication and PoE supply, auxiliary power supplies as required by environmental housings, plywood backboards, necessary software, programming and commissioning.
- .2 Provide IP visible and near visible spectrum cameras at the designated locations as shown on the drawings.
- .3 Provide network switch for communication and camera power supply over PoE/PoE+/hPoE/hPoE+ with capacity based on the noted project equipment matrix and design layouts sized to suit the total connected camera load plus 50% PoE capacity and 25% port capacity to allow for future expansion.
- .4 All cabling to meet City of Brampton standards stated in section 1.3.3.
- .5 Ensure equipment manufacturer provides all information regarding wiring, conduit runs and component requirements before tendering. City will not be responsible for added costs and changes due to additional manufacturer's requirements.
- .6 All NVRs shall be housed in the designated lockable cabinet at the location shown on the drawings. All net new cabinets to provide 50% spare rack space, measured in rack units (U) to allow for system expansion.
- .7 Vendors must notify the City immediately if the installation of a camera will exceed 90 meters from the location of its installation to the location where it is connected to the network switch for this project, unless the use of ethernet extension technology are specified for the specific camera already.
- .8 The vendor shall all engage in all commercially reasonable efforts to supply and install edge devices that have undergone the following configuration hardening as a minimum standard:

- .1 Disabling any non-encrypted communication protocols i.e. FTP/21, SMTP, POP server access, web access via port 80, etc.
- .2 Updating default administrator passwords
- .3 Disabling any device discovery protocols and SNMP
- .4 Enabling secure communications protocols i.e. HTTPS via SSL, SecureFTP via SSH, etc.

2.5 Intrusion Detection System General Requirements

- .1 Supply and install a complete and operational intrusion alarm system consisting of alarm panels, door contacts, motion sensors, interface accessories, interface hardware, power and signal cables, conduits, wireways, power supplies, necessary software, programming and commissioning.
- .2 Systems shall be as shown on the drawings and herein specified.
- .3 All wiring for the intrusion alarm system shall be run in conduit, unless otherwise indicated on the drawings or advised by the City of Brampton Corporate Security Services and shall be concealed in finished areas.
- .4 The normal power supply to the intrusion detection system shall be 120 Volts 60 HZ taken from the building service at the closest panel. Provide new breaker in existing panel to match existing breakers if required. Power from the building service shall be dedicated to the intrusion detection system and not shared by any other system.
- .5 Ensure equipment manufacturer provides all information regarding wiring, conduit runs and component requirements before tendering. Owner will not be responsible for added costs and charges due to additional manufacturer's requirements.
- .6 The vendor shall all engage in all commercially reasonable efforts to supply and install edge devices that have undergone the following configuration hardening as a minimum standard:
 - .1 Disabling any non-encrypted communication protocols i.e. FTP/21, SMTP, POP server access, web access via port 80, etc.
 - .2 Updating default administrator passwords
 - .3 Disabling any device discovery protocols and SNMP
 - .4 Enabling secure communications protocols i.e. HTTPS via SSL, SecureFTP via SSH, etc.

2.6 Intercom System General Requirements

- .1 Supply and install a complete and operational intercom system consisting of one or more of the following items: master stations, client stations, interface accessories, interface hardware, power and signal cables, conduits, wireways, power supplies, necessary software, programming and commissioning.
- .2 Systems shall be as shown on the drawings and herein specified.
- .3 All wiring for the intercom alarm system shall be run in conduit, unless otherwise indicated on the drawings or advised by the City of Brampton Corporate Security Services and shall be concealed in finished areas.
- .4 Ensure equipment manufacturer provides all information regarding wiring, conduit runs and component requirements before tendering. Owner will not be responsible for added costs and charges due to additional manufacturer's requirements.
- .5 Provide network switch for communication and intercom client/master station power supply over PoE/PoE+/hPoE/hPoE+ with capacity based on the noted project equipment matrix and design layouts sized to suit the total connected camera load plus 50% PoE capacity and 25% port capacity to allow for future expansion.

2.7 Network Switches General Requirements

- .1 The vendor shall all commercially reasonable efforts to supply and install switches that have undergone the following configuration hardening as a minimum security standard:
 - .1 Disabling any non-encrypted communication protocols i.e. FTP/21, SMTP, POP server access, web access via port 80, etc.
 - .2 Updating default administrator passwords
 - .3 Disabling any device discovery protocols and SNMP
 - .4 Disabling VLAN 1
 - .5 Enabling secure web communications via SSL and secure remote session access via SSH
 - .6 Disabling any unused ports
 - .7 Configuring any connected ports with MAC address access list for the connected device
- .2 Systems shall be as shown on the drawings and herein specified.
- .3 Provide network switches that allow for capacity expansion above and beyond the total connected camera load at the time of installation. Additional capacity

to be defined as 50% additional PoE capacity and 25% additional port capacity to allow for future expansion.

- .4 Where available switches will be configured to utilize connection resiliency protocols such as LACP for connections to servers and inter-switch links to maximize connection and device uptime.

2.8 Network Media Extenders General Requirements

- .1 Supply and install network media extenders that meet the following criteria:
 - .1 Available in multiple form factors from single channel through high density rackmount solutions.
 - .2 Support both copper and fibre media.
 - .3 Rackmount solutions to provide 25% expansion capacity for adding new connections.
- .2 Systems shall be as shown on the drawings and herein specified.

2.9 Backup Power Supplies General Requirements

- .1 Supply and install backup power solutions that meet the following criteria:
 - .1 Rack mountable in standard 19 inch rack/enclosures
 - .2 Provide 15 minute runtime for all connected devices mounted in the rack
 - .3 Provide 25% expansion capacity for new devices.
 - .4 Support network management and monitoring via an installed or embedded network monitoring card for all UPS's supporting all Windows/Linux server installations and 16 and 32 channel rackmount NVR applications. UPS application supporting 8 channel NVRs and workstations/PCs do not require network monitoring capability.
- .2 The vendor shall all engage in all commercially reasonable efforts to supply and install edge devices that have undergone the following configuration hardening as a minimum standard:
 - .1 Disabling any non-encrypted communication protocols i.e. FTP/21, SMTP, POP server access, web access via port 80, etc.
 - .2 Updating default administrator passwords
 - .3 Disabling any device discovery protocols and SNMP
 - .4 Enabling secure communications protocols i.e. HTTPS via SSL, SecureFTP via SSH, etc.
- .3 Systems shall be as shown on the drawings and herein specified

2.10 Equipment Room Fittings General Requirements

- .1 Supply and install equipment racking solutions that meet the following criteria:
 - .1 Full height (37U), half height, and wall mount configurations.

- .2 Full height and half height racks to be 27 inch depth to allow for the installation of up to 22 inch depth network appliances.
 - .3 Provide 25% expansion capacity, measured in rack units (U) for the installation of new devices.
 - .4 At a minimum will include:
 - .1 Locking front and rear doors.
 - .2 Removable side panels
 - .3 Active ventilation
 - .4 Cabling management
 - .5 Rack chassis mounted vertical power distribution strips
 - .5 Provide thermal output calculations for all hardware installed in the rack to ensure adequate active ventilation is provided with the rack.
- .2 Systems shall be as shown on the drawings and herein specified

2.11 Computers and Servers General Requirements

- .1 The vendor shall all commercially reasonable efforts to supply and install laptops, workstations, and servers that have undergone the following configuration hardening as a minimum security standard:
 - .1 Disabling any non-encrypted communication and file sharing protocols i.e. uPnP, Windows File Sharing
 - .2 Updating default administrator account passwords
 - .3 Apply all available O/S updates
 - .4 Install and update antivirus/antimalware application
 - .5 Lock down system BIOS with a password
 - .6 Disable all remote boot options in BIOS i.e. PXE, USB
 - .7 Ensure all built-in Windows Exploit protections are enabled for Windows 10 O/S machines.
 - .8 Apply all system hardening patches, fixes, and updates as specified in security application provider system hardening guides and the Center for Internet Security (CIS) server hardening guidelines.
- .2 Systems shall be as shown on the drawings and herein specified.
- .3 Provide three (3) year next day onsite support warranty for all laptops and workstations.
- .4 Provide five (5) year four (4) hour onsite support warranty for all servers.
- .5 All computers, workstations, and laptops shall utilize solid state hard drives for the primary O/S drive.
- .6 All storage arrays will exclusively be equipped with enterprise rated hard drives. Acceptable manufacturers are HGST (Hitachi), WDC, Toshiba, and Seagate.

Section 3 Accepted Part Numbers by System Type

3.1 The following are the acceptable Access Control Management System components and hardware:

Manufacturer	Item Description / Part Number
RBH	UNC-500-822M
RBH	RC2M Reader Controller
RBH	IOC-16 Input Output Controller
RBH	ENCL1-PS
RBH	ENCL2-PS
ATC Frost	TCE150161 16VAC 150 VA Transformer
Tyco/DSC	PC-100 ASCII Gateway for DSC intrusion alarms
Camden Door Controls	Camden CX12
Camden Door Controls	Camden CX 32
Camden Door Controls	Camden CX WEC13
Dorma Kabba	RCI 8310/8320 Mag-lock
Assa Abloy	HES 1600 CLB Complete Pack
Assa Abloy	HES 9600
Assa Abloy	HES 5200
Assa Abloy	HES 9400
Assa Abloy	HES 1006 CLB Complete Pack
Assa Abloy	HES 9500
Assa Abloy	HES 9400
Assa Abloy	HES 9600
HID	Multiclass RP-40 Multi-card Reader 920PTNNKO

3.2 The following are the acceptable Network Video Recorders:

Manufacturer	Item Description/Part Number
March Networks	8732 with 4 X 6TB
March Networks	8708 With 2 X 6TB
March Networks	8704 with 2 X 4TB
March Networks	9132 with 40TB of Storage
March Networks	9248 with 80TB of Storage
March Networks	9264 with 80TB of Storage

3.3 The following are the acceptable analog and IP CCTV cameras and accessory equipment:

Manufacturer	Part Number
Axis Communications	M3026-VE
Axis Communications	Q6000-E MK II
Axis Communications	M5525-E
Axis Communications	P3225 MKII
Axis Communications	P3225-LVE MKII
Axis Communications	M3044-V
Axis Communications	T8133
Axis Communications	T8134
Axis Communications	T94AO1D
Axis Communications	T91A64
Axis Communications	T91D62
Axis Communications	T91L61
Panasonic	Panasonic WV-X6531N
Panasonic	Panasonic WV-S2531LN
Panasonic	Panasonic WV-SFN480
Panasonic	Panasonic WV-SFV481
Panasonic	Panasonic WV-Q122A
Panasonic	Panasonic WV-Q124
Panasonic	Panasonic WV-Q121B

3.4 The following are the acceptable intrusion detection systems equipment and accessories:

Manufacturer	Item Description / Part Number
Tyco/DSC	PC1864NK Control Panel with Large Cabinet
Tyco/DSC	3G2060R GSM Communicator
Tyco/DSC	PK-5500 LCD
Tyco/DSC	DSC-BV500GB
Tyco/DSC	PC5108
Interlogix	1078
Interlogix	1085T
Potter	ODC59A
Bosch	ISCPR1W6
ATC Frost	FTC3716
Eyez On	EVL4CG

3.5 The following are the acceptable intercom stations and accessories:

Manufacturer	Item Description
Commend	ES833A
Commend	ES831A
Commend	ES2GBB
Commend	ES2GRH
Commend	Intercom Server GE 800
Commend	Intercom Server GE 300
Commend	ET901WP
Commend	G3-IP-4B
Commend	G3-GED-4B
Commend	G8-IP-4B
Commend	L8-IP-8B
Commend	L8-IP-8P
Commend	ES2GBB
Commend	L8-ICX
Commend	G8-LAN-8
Commend	L8-LAN-16
Sentrol	GE3040
Safety Technology International	SS2472EM-EN

3.8 The following are the acceptable managed PoE/PoE+ network switches:

Manufacturer	Item Description/Part Number
Cisco Systems	Cisco SG300-10P
Cisco Systems	Cisco SG110-24HP
Cisco Systems	Cisco SG300-28P

3.9 The following are the acceptable cable types:

Manufacturer	Item Description/Part Number
Provo	Network - 9924104L5E-350GN FT6
Provo	Access Control – 8913 FT4
Provo	Access Control – 998913 FT6

3.11 The following are the acceptable uninterruptible power supplies, communication modules, and replacement batteries:

Manufacturer	Item Description
APC by Schneider Electric	SMT1500RM2UC
APC by Schneider Electric	AP9630
APC by Schneider Electric	BR1500G
APC by Schneider Electric	RBC115
APC by Schneider Electric	RBC124
APC by Schneider Electric	RBC133

3.12 The following are the acceptable equipment rack part numbers and ancillary racking equipment:

Manufacturer	Item Description/Part Number
Middle Atlantic	DWR-10-22
Middle Atlantic	DWR-16-22
Middle Atlantic	DWR-24-22
Middle Atlantic	WRK-37SA-27
Middle Atlantic	VFD-10
Middle Atlantic	VFD-16
Middle Atlantic	VFD-24
Middle Atlantic	LVFD-37
Middle Atlantic	QFP-2 / 1
Middle Atlantic	QFP-2 / 2
Middle Atlantic	U2 / 1
Middle Atlantic	RLNK-SW815R-SP
Middle Atlantic	PD-815SC

3.13 The following are the acceptable laptop, workstation, server, and data storage unit product lines:

Manufacturer	Item Description / Part Number
Dell	Latitude and Precision Workstation Laptops
Dell	Optiplex Desktops Precision Fixed
Dell	Power Edge Rack Mount Servers
Dell	PowerVault Storage Appliances
HP	zBook Workstation Class Laptops
HP	Z Series Workstations
HP	Hp ProLiant Servers and Storage Arrays

Section 4 – System Specifications

28 10 00 Access Control

28 23 00 Video Surveillance

28 30 00 Security Detection, Alarm and Monitoring

28 50 00 Specialized Systems – Intercom Entry Systems

26 33 00 Battery Equipment

27 11 00 Communications Equipment Room Fittings

27 20 00 Data Communications

27 22 00 Data Communications Hardware

General Purpose

- 1.1.1. To establish the technical, functional, jurisdictional, or regulatory and quality requirements for security and access control systems; which are required to be purchased from vendors. Approved technical specifications define the supply and installations of all security and access control systems and identify approved manufacturers and models.
- 1.1.2. The security system shall consist of implementing an integrated networked Access Control and Video Assessment System (ACAMVAS) that shall control personnel access, provide real time intrusion detection alarm monitoring and provide alarm driven video surveillance for the designated buildings and operations in accordance with the requirements and specifications prescribed in these documents and the approved drawings. The security system shall include the following, where applicable:
 - 1.1.2.1. Seamless integration of a digital video management system that will allow system operators to control and maintain the security of the facilities from multiple designated client workstations.
 - 1.1.2.2. Seamless integration of video surveillance systems that provides alarm driven assessment for the intrusion detection equipment at designated facilities.
 - 1.1.2.3. Seamless integration with wireless networked locksets from Assa Abloy or Salto to provide doors with a battery powered solution for access control without the need to pull multiple wiring cables to the door.
 - 1.1.2.4. Commissioning and testing of the systems and equipment installed as required to meet manufacturers' specifications and documented installation procedures, and to the satisfaction of the Owner.
 - 1.1.2.5. Training of the Owner's personnel to: fully operate, and perform routine maintenance on the systems and equipment installed.
 - 1.1.2.6. Provide all associated documentation for the security system upgrades.

1.2 Reference Standards

Underwriters' Laboratories of Canada (ULC)

- 1.1.2.7. American National Standards Institute (ANSI) Standards
- 1.1.2.8. Ontario Building Code
- 1.1.2.9. CANASA (Canadian Alarm and Security Association)
- 1.1.2.10. CFAA (Canadian Fire Alarm Association)

All products comply with the Canadian certifications listed above.

PRODUCTS

SECURITY COMPONENTS

1.1.3. Listed below are the security components that shall be supplied and installed. A detailed specification of each of the security components included in this list is also included.

ACCESS CONTROL AND ALARM MONITORING SYSTEM

General System Specifications

The access control and alarm monitoring system shall be the RBH Access Technologies AxiomV Enterprise system and meets the following design and performance specifications:

- 1.1.3.1. The system shall be a modular, networked access control and alarm monitoring system, comprised of proven commercial off the shelf components, capable of handling large proprietary corporations with multiple remote sites, alarm monitoring, video imaging, badging, paging integration, CCTV integration, interactive guard tour, mapping, visitor management, email notification, third party monitoring, BAS integration and asset management. The system shall assure long time performance, cost effective upgrade capability and allow for easy expansion or modification of inputs, outputs and remote control stations.
- 1.1.3.2. The system control at the central computer location shall be under a single software program control, shall provide full integration of all components, and shall be alterable at any time, depending upon the requirements. Reconfiguration shall be accomplished online through system programming, without hardware changes.
- 1.1.3.3. The Access Control Software system shall utilize Microsoft SQL Server 2008/2012/2016 for data storage and be written expressly for Microsoft SQL Server 2008/2012/2016.
- 1.1.3.4. The system shall have the capability to be networked via a LAN/WAN connection utilizing industry standard TCP/IP communication protocol. The system shall provide encryption via the TCP/IP connection
- 1.1.3.5. The system shall incorporate the use of bi-directional 485 communications and/or Class "A" TCP/IP redundant connections for redundancy and reliability.
- 1.1.3.6. The system shall incorporate "High Availability" Communications so that multiple communication paths are available to all controllers. High availability shall be defined as, "an existing alternate controller shall take over communications in the event the main controller fails. The controller must be located in a separate location to the first."
- 1.1.3.7. The system shall support both manual and automatic responses to alarms entering the system. Each alarm shall be capable of initiating a number of different actions, such as camera switching, activation of remote devices and door control.

- 1.1.3.8. The system shall provide unlimited levels of emergency codes to allow the system to operate in different security levels depending on local threat level e.g. code black = bomb threat and building locks down.
- 1.1.3.9. The system shall provide both supervised and non-supervised alarm point monitoring. Upon recognition of an alarm, the system shall be capable of switching CCTV cameras and automatically creating a popup window for video for the associated alarm. The system shall be capable of arming or disarming alarm points both manually and automatically, by time of day, and by day of week.
- 1.1.3.10. Access control functions shall include validation based on time of day, day of week, holiday scheduling, site code verification, automatic or manual retrieval of card/tagholder photographs, and access validation based on positive verification of card/tag, card/tag/PIN, card/tag and video.
- 1.1.3.11. The system programming shall be user friendly, and capable of being accomplished by personnel with no prior computer experience. The programming shall be menu driven and include online "Help" with the use of F1 hotkey to automatically call the proper help information to the screen. The software shall utilize drop boxes for all previously entered system required data.
- 1.1.3.12. After installation, the Owner shall be able to perform basic hardware configuration changes. These hardware configuration changes shall include, but not be limited to, door open time, door contact shunt time, point and reader names, when and where a card/tagholder is valid, and the ability to add or modify card/tag databases as desired without the services of the Manufacturer or Manufacturers Dealer.
- 1.1.3.13. Equipment repair shall be able to be accomplished on site, by module replacement, utilizing spare components. All equipment shall have pluggable connectors for easy replacement.
- 1.1.3.14. All control components shall include the ability to download operating parameters to any control panel, thus allowing the control panel to provide full operating functions independent of any other system component.
- 1.1.3.15. The system shall be designed in such a way that it does not require enrolment of authorized personnel at each building.
- 1.1.3.16. The system shall provide seamless integration to multiple manufacturers of DVR's and NVR's at the same time.
- 1.1.3.17. The system shall provide seamless integration with external building control systems (BAS), personal safety systems, remote paging and email systems.
- 1.1.3.18. All system events, operator actions and maintenance information shall be stored on the computer hard disk to maintain a permanent record of system activity. The system shall have the capability for manual and automatic back-up of set-up and

system events to either local removable media (optical/magnetic) or remote network resource.

1.1.3.19. All workstations shall be configurable to act as Alarm monitoring centre for the system. All alarms shall be configurable by schedule and workstations will have the ability to acknowledge and clear alarms as a two step process.

1.1.3.20. All workstations shall have the ability to define alarm routing with an unlimited number of Routing levels available to the system.

1.1.4. Interactive Mapping and Graphics

The system shall support an unlimited number of user programmable colour graphic map displays capable of showing the floor plan, location of alarm device, and alarm instructions. Floor plans shall be created in an approved format and shall be capable of being imported from other systems. All of the graphic maps shall be displayed on the CPU monitor. Systems requiring separate display monitors or PC's shall not be acceptable. Maps shall be interactive with dynamic real-time status so that the operator can control all device functions from the map.

1.1.5. Information Storage

All programmed information as well as transactional history shall be automatically stored onto the hard disk for later retrieval.

1.1.6. Information Backup/Retrieval

The CPU shall be capable of transferring all programmed data and transactional history to thumb drive or any logical disk drive. All programmed data shall be restorable from disk in case of system hardware failure.

1.1.7. Communication Rates

The system shall have bi-directional communications and communicate up to 2.5mb/s.

1.1.8. Printers

The system shall support all system printers configured under and supported by the Windows ® operating system.

1.1.9. Pointing Device

The system shall use the pointing device configured under and supported by the Windows ® operating system.

1.1.10. Communication Ports

The system shall support an unlimited number of either serial or TCP/IP ports.

1.1.11. Workstations

The system shall support an unlimited number of active remote workstations. These stations shall be capable of monitoring alarms and changing the database and retrieving transaction records in real time without affecting the other stations.

1.1.12. Networking

The system shall operate with the standard Windows ® networking software.

1.1.13. Database

The database shall be Microsoft SQL Server 2008/2012/2016.

1.1.14. Software Capacities

1.1.14.1. The System server shall have the following minimum requirements. Server 2008/2012, Windows 7, 8.1 and 10 pro, with 2.2 GHz clock speed, 2gig Ram, 40 gig hard drive, CD Rom, Pointing device and video graphics card with 512 on board ram.

1.1.14.2. System software and language development software shall be existing, industry accepted, and of a type widely used in commercial systems. The solutions operating system requirements shall be as identified in 2.2.3. The application software shall have been written in a standard, industry accepted language. All System functions shall be accessible via Windows ® operating systems compliant menu accessed screens. Systems requiring command string control or complex syntax shall not be acceptable. Systems shall not be dependent upon external input other than keyboard.

1.1.14.3. The system software shall include the following features and be configured as a minimum:

- Unlimited reader expansion
- Unlimited card/tagholders in software
- Unlimited simultaneous client PCs
- Unlimited time zones
- 365 user-definable holidays
- Unlimited Access levels
- Access levels for each card/tagholder
- Unlimited alarm input points
- Unlimited output control points
- Unlimited operator passwords with definable privilege levels
- Audible alarm annunciation at the CPU
- Unlimited colour graphic maps displayed on the CPU monitor
- TCP/IP or RS232 interface capability to a CCTV system, which provides automatic, alarm actuated camera switching.

- True 32/64 bit operation
- Operator activation/cancellation dates
- Employee activation/cancellation dates
- Optional Video Imaging/Badging & bar code imprinting

1.1.15. System Administrators shall have the following abilities as a minimum:

- To change any station settings from whatever station they are working on.
- To establish Station Names. Station names shall be user-definable.
- The Station Status dialog shall be available. It shall display a list of stations and their on-line/offline status, along with the names of the logged-on operators.
- Report Printers: Reports as requested by the operators are sent to printers that may reside anywhere on the network.

1.1.16. Alarm Window Description

The system shall facilitate the processing of alerts by using a pop-up alarm window. The Window shall list the system alarms and allow the operator to acknowledge and clear by right-clicking on the event. The alarm window shall indicate time of alarm and response time by the operator. The alarm shall incorporate programmable instruction messages to instruct the operator what he is to do. The alarm will also have an operator action window to log an action into history for the alarm.

1.1.17. Bulk Acknowledgment of Alarms

The system shall provide a means to bulk-acknowledge alarms, so that all alarms can be acknowledged with a single operator action.

1.1.18. Station Routing

The system shall support the routing of alarms to any or all stations. Time schedules can be used to determine which station an alarm is routed to at what time. An alarm may be routed to one station or group of stations during a time schedule and re-routed to another station or group of stations during another time schedule.

1.1.19. Operator Routing

The system shall support the routing of alarms to particular operators, regardless of which station the operator is logged onto.

1.1.20. Menu Configurations

The system software shall allow for the configuration and programming of the controller panel through the use of a simple graphical user interface (GUI). All devices and functions shall be right click configurable for easy operation.

1.1.21. Memory

Memory within each controller panel shall be automatically configured by the system.

1.1.22. Database Updates

The system software shall download/upload information to the controller panels automatically while the controller panels are in communication with the host CPU. A data download may also be initiated manually.

1.1.23. Reporting

The system software shall have the capability to report selectable data by type and by time zone. The system software shall allow the user to generate a report to screen, to printer or to save to a file. The reports shall be exportable to over 30 different file formats. The system shall incorporate the use of an automatic report generator.

1.1.24. Workstations

The system software shall have the capability to report selectable data by type and by time zone to any combination of the system workstations simultaneously.

1.1.25. Serial Ports

All serial ports shall be configured from an easy to follow menu. Systems requiring in depth knowledge of the operating system or CMOS setup for port configuration shall not be acceptable.

1.1.26. Time Zones

1.1.26.1. The system software shall have the capacity for a minimum of 255 user-definable time zones. Each time zone shall allow for a minimum of 16 individual time intervals.

1.1.26.2. The time zones shall be assignable to:

- Card/tagholders
- Outputs
- Alarming reporting functions
- TCP/IP and RS232 message ports
- Doors
- Reports
- Printer operation
- Workstations

1.1.27. Holidays

The system software shall support a minimum of 365 holidays. Holidays shall be considered H1 or H2 designation so that there are three distinct holiday times. A holiday shall be capable of starting at any

time/hour during a 24-hour day. Systems requiring holiday start time of midnight shall not be acceptable.

1.1.28. Door Descriptions

Each door in the system shall be identified using logical tagging format and approved by the Owner. Each door description shall be assigned user-definable text of up to 50 characters.

1.1.29. Access Control Modes

Each door may be programmed to switch automatically based on a user defined time schedule between the following modes of operation:

- "CARD/TAG ONLY"
- "CARD/TAG + PIN" – Dual authentication shall be provided for access points requiring the user to use their credential and enter a four digit PIN number.
- "PIN ONLY" – Keypad readers shall be used at doors to prevent access by Alzheimer residents.
- "HIGH SECURITY"
- "TWO PERSON" - To add additional security two people must be required to present cards (or any other credentials) in order to access a secure area.
- "FREE ACCESS"

1.1.30. Duress

If the reader is operating in the "CARD/TAG + PIN" mode or "PIN ONLY" mode, a duress feature shall allow an alternate code to be entered into the keypad for access. The system shall generate an alert and may be linked to control relays for notification of the alarm.

1.1.31. Door Alarms

Each door may be programmed to generate "FORCED DOOR" and "DOOR HELD OPEN" alarms. These alarms shall have the ability to have a user-definable time delay.

1.1.32. Door Alarm Annunciation

In addition to generating an alarm message, the following conditions may activate an output for annunciation:

- FORCED DOOR
- DURESS
- DOOR HELD OPEN (DOOR AJAR)
- VOID CARD/TAG
- DENIED CARD/TAG
- ANTI-PASSBACK VIOLATION

- INPUT DOOR ALARM
- TAMPER
- ALARMS

1.1.33. Alarm Description

Each alarm point may be defined with a plain text description of up to 50 characters.

1.1.34. Alarm Enabling

Alarm points shall be enabled during user-definable time zones and may be manually enabled/disabled from any workstation.

1.1.35. Additional Alarms

The system must also generate alarms for the following:

- Enclosure tampering
- Controller panel communication loss
- Channel 1 Fail /Channel 2 Fail
- Battery Failure
- AC Failure
- Reader Fuse
- Auxiliary Fuse
- Lock Fuse
- Alarm tampering (supervised)

1.1.36. Alarm Supervision

When using supervised alarm points, the system must monitor for “OPEN”, “SHORT”, in addition to “NORMAL/ABNORMAL” conditions.

1.1.37. ASCII Output:

Alarm points shall output an ASCII via RS232 or TCP/IP text command for integration to any other IP commandable device. This command/output shall be an optional, user-definable and transmitted on alarm points going into abnormal state, returning to a normal state, or both.

1.1.38. Outputs

- 1.1.38.1. Shunt relays: User definable outputs may be assigned as shunt relays, allowing access doors to be monitored by third party alarm systems.

1.1.38.2. Relay “on” time: Outputs assigned to control doors shall be user-definable from 1-127 seconds or minutes.

1.1.39. Encryption

The passwords shall be encrypted in the operator database using encryption, to facilitate confidentiality of individual operator passwords.

1.1.40. Operator Access Levels

The system shall provide unlimited operator access levels for the system. All operator actions will be recorded within the system database.

1.1.41. Password Security

The Operator password shall be encrypted to prevent operators from seeing passwords. Passwords shall be up to 20 alphanumeric characters and be case sensitive. Operators must have the right to edit their own password for secrecy.

1.1.42. Partitioning

The System shall incorporate true database partitioning by operator. An operator shall logon anywhere on the system and have the same functionality at any workstation. Operators will be limited to see and control of the system by their operator Access level.

1.1.43. Operator Access Levels

The system shall have the ability to define unlimited user roles. As a minimum, the user roles shall be:

- General Administrator
- Supervisor
- General User
- Privilege levels shall be assignable to, but not limited to the following menu functions:
- View
- Edit
- Edit of any field within the menu
- Select

1.1.44. Operator Activity

All operator activity including specific changes to the database shall be stored for later retrieval and Operators shall be assigned a time zone for the purpose of logging in.

1.1.45. Audit Trail of Database Changes

1.1.45.1. The system shall record changes to the database, including the date, time, operator name and description of the record changed.

1.1.45.2. The audit trail event messages shall record additions, deletions and revisions. The record shall contain a date/time stamp for the change, the logged on operator's name, the table name, a character identifying the change, and a description based upon the Name field from the record, such as the user name, operator name, panel name, reader/door name.

1.1.45.3. The system shall do a full restore or partial depending on operator selection of the data or history files during the back-up process.

1.1.45.4. The system shall allow for viewing of the audit trail.

1.1.45.5. The system shall NOT allow The Audit Trail table to be edited.

1.1.46. Employee Definitions

1.1.46.1. Card Entering:

Card entering shall be easy so that minimal training is required. Card input and changes shall be allowed through direct interface with the event viewer screen. Cards shall have the ability to have multiple access levels or assigned special access levels. Cards may be inactivated from the system while the data remains for reactivation at a later date.

1.1.46.2. Card/tag Data:

The system software shall allow for card/tag numbers up to 18 digits.

1.1.46.3. Employee records:

Employee records shall consist of a minimum of the following:

- Card/tag Number
- Issue level
- Two (2) groups of access level and time zone
- User-definable PIN code
- Facility code
- Anti-passback location and status
- Expiration date
- High Security
- Lock/Unlock privilege
- Code Links
- Track status

- Last door accessed
- 22 user definable searchable text and data fields
- Duration use
- Escort
- Extended shunt (for ADA compliance)
- Passback override

1.1.46.4. Batch Loading:

The system software shall allow groups of card/tags to be input through the use of a card/tag number range or by a batch load employee field.

1.1.47. Reports

1.1.47.1. Data Storage:

All programmed and transactional history is automatically stored to the hard disk for later retrieval.

1.1.47.2. System Function:

The system software shall be capable of generating reports without affecting the real-time operation of the system.

1.1.47.3. Media:

Reports shall be generated from the hard disk, or removable media and exportable to over 30 file formats.

1.1.47.4. Search Criteria:

The database shall be structured such that the operator shall determine the search parameters based on variables available on the individual report menu. Systems requiring the user to type complicated search strings shall not be acceptable.

1.1.47.5. Report Types:

User-definable data reports shall be available for the following information:

- Card/tagholder data
- Door groups
- Time zones
- Doors
- Inputs
- Relays

- Links
- Controller panels
- Operators
- System hardware configuration
- System settings configuration

1.1.47.6. Transaction Reports:

Transaction reports shall be available for the following:

- Card/tag transactions
- Alarm transactions
- Event transactions
- Operator activity
- Time and Attendance

1.1.47.7. Report Scheduling:

The system software shall have the ability to batch reports to any of: screen report, report to a network printer or save a report to a file without operator initiation.

1.1.48. System Guides

1.1.48.1. On Line Help:

The system software shall have on line help available at any point requiring operator input. The help screen shall be accessible by using the standard Windows ® help systems. These help screens shall contain context sensitive information that shall allow the operator to enter correct data without consulting the manual. The help menu shall be accessible to the exact point in software by using the “F1” hotkey.

1.1.49. System Status

1.1.49.1. Real Time Status:

The operator shall be able to monitor via graphical screens, the status of the following in real time:

- Inputs
- Outputs
- Doors

1.1.49.2. Alarm Monitor:

A screen shall be available to monitor alarms and view, at minimum, 99 of the most recent events. The operator shall also have the ability to view additional detail of any event through the use of a single keystroke or click of the mouse.

1.1.50. Graphics

1.1.50.1. Graphics File Format:

The floor plans shall be configured in AutoCAD, JPEG or Bitmaps.

1.1.50.2. Programming:

The system software shall be able to import floor plans produced in AutoCAD.

1.1.50.3. Operation:

Upon activation of a selected input or door alarm the map shall pop-up and display the alarmed device with an alarmed icon. The operator shall be able to click on the map and clear the alarm or control the device from the graphical interface. Mapping shall be realtime and interactive.

1.1.51. Video Badging

1.1.51.1. The system shall have the capability to permit Video Imaging and Badging, which shall, when used in conjunction with the system software, function as an integrated Video Imaging/Badging and access control system. The system shall utilize a single PC to input data for both access and video Badging. The system shall not require the operator to enter data more than once. Badge information including name, card/tag number, signature, fingerprint, user text, bar coding and up to five data fields shall be available for each card/tag. The system shall provide for user definable backgrounds. These backgrounds may be a "captured" image or a colour background. The system shall be capable of supporting Windows ® 2000/XPPRO/WIN7PRO compliant video printers.

1.1.51.2. Badges may be created in both horizontal and vertical configurations. In order to change a card/tagholder's badge, a new background may be selected from the background table. A new picture capture is not required. The system shall allow any input or reader to be programmed such that an event at that location is captured by a remote camera and displayed while being stored in the database for later viewing or printing. Events at the reader shall display in real time and store a "split screen" showing the stored card/tagholder image next to the "captured" image. Camera control shall be accomplished via an RS232 interface from the system to a video switcher. The programming of the camera switcher for the individual inputs and readers shall not require exiting from the access control program.

1.1.51.3. Additional Badging and/or alarm PC stations may be added via a local area network (LAN).

1.1.52. Video Imaging

1.1.52.1. The system shall have the capability to import images of employees and store them in the database. These images may be recalled and displayed by the operator.

- The system shall have the ability to capture pictures and save from IP Video Cameras.

- The system shall provide for the backing up and restoral of captured pictures.

1.1.53. DVR and NVR Integration

- 1.1.53.1. The system shall be able to integrate seamlessly via TCP/IP to multiple manufacturers DVR's and NVR's simultaneously. The operator shall have the option to associate any camera with a device and through a common video window, control, and operate any device with real time viewing. Video shall be accessible from any device via a right mouse click.
- 1.1.53.2. Video history of any event shall be accessible via a right mouse click.
- 1.1.53.3. The video window shall automatically pop-up upon activation of the associated device's alarm. Video shall be common to all manufacturers systems so that the operator only sees one view.
- 1.1.53.4. Non-proprietary servers shall be used with provision for fail-over and redundancy.
- 1.1.53.5. VMS shall be available in multiple languages including French.
- 1.1.53.6. The VMS (video management software) shall be compatible to ONVIF compliant cameras and many other IP cameras.

1.1.54. Interactive Guard tour:

The system shall incorporate an interactive guard tour module to provide real time status of the Guards progression. Failure to complete a tour shall activate alarms on site and off-site for life safety operations.

1.1.55. Asset Management:

The system shall incorporate an asset management module so that owners are assigned to equipment or vehicles to prevent theft. Upon alarm the system shall notify via alarm, CCTV interface, and email status the improper event.

1.1.56. System Tools

- 1.1.56.1. Copy Wizard -The system shall provide a copy wizard to quickly copy any device parameter to any other single or group of devices.
- 1.1.56.2. Back-up Scheduler- The system shall have a backup scheduler for automatic backup of data
- 1.1.56.3. Custom Cardholder fields - The system shall have the ability to custom design the cardholder data by adding new fields at will.

1.1.57. Biometric/Fingerprint Enrollment

The software shall have an integrated tab in the cardholder screen to enable the operator to enroll fingerprints/ biometrics directly from the software. Programs that open third party software are unacceptable.

Hardware - AxiomV Controller Panels

UNC500 TCP/IP CONTROLLER

- 1.2. The controller panel shall be a 32 bit microprocessor controlled solid-state electronic device and shall include a real time clock/calendar on board. Boards shall be made of gold plated construction (Copper or leaded will not be accepted) and incorporate flashware technology. Communication shall Two channel TCP/IP standard LAN/WAN windows environment protocol. A subset of the system database sufficient to support access and alarm functions for its designated readers and points shall be stored at the controller panel. In event of communication loss, the controller panel shall continue to function without degradation of operation and shall provide storage of a least 10,000 events. These stored events shall be uploaded to the CPU automatically upon restoration of the communications. The system shall be capable of performing all system functions indefinitely without the computer.
- 1.3. The controller must be FCC, CE, RoHS and UL listed.
- 1.4. The controller must have 8mb Ram available on board
- 1.5. The controller must have 65,000 offline event buffer
- 1.6. The controller must have 3 programmable RS485 ports
- 1.7. The controller must have 2 on board Wiegand reader ports to accept any Wiegand format and 5 Wiegand formats simultaneously.
- 1.8. The controller must have 8 fully supervised inputs capable of individual configuration for EOL (single and dual EOL), N.O, N.C. operation.
- 1.9. The controller must have 8 outputs. 4-form 'C' relay outputs rated at 10A-30VDC and 4-open collector 100ma outputs.
- 1.10. The controller must have two on board TCP/IP LAN connections capable of configuration in LAN switch mode or dual LAN operation for Class 'A' Communication configurations.
- 1.11. The Controller must have separate tamper input
- 1.12. Input voltage 12vdc or 30w P.O.E. maximum current draw 500ma
- 1.13. The controller must have internal charging circuit for 12vdc gel cell standby battery. The controller shall be capable of recharging a standby battery from either P.O.E. source or 12v local power supply.
- 1.14. The controller shall be configurable in the following methods. Edge device, Wall mount controller or Rackmount.

- 1.15. Edge device deployment shall be POE and operate continuously even if POE is lost. Edge controller shall operate 1 or 2 doors as desired.
- 1.16. Rackmount configuration shall be 2 UNC500 controllers or 4 doors in a standard 1U-19inch rack configuration. LAN connections shall be front facing as standard Network configuration. All device connections shall be independent and removable from the rear of rack for quick disconnect and easy troubleshooting. All rackmount cabinets shall have optional rails for slide out configuration. All rackmount cabinets shall have top removable panel to access control panels.
- 1.17. The controller when configured in switch mode shall allow LAN looping from one standard windows device to another as any standard network switch allows without the use of external switches or special LAN cabling.
- 1.18. The controller must accept and control up to 7 slave reader controllers and 16 I/O controllers simultaneously.
- 1.19. Links are defined as any action causing any reaction on the system. Each controller shall be capable of initiating 'Links' regardless of the computer status.
- 1.20. Readers shall have the ability to initiate s swipe and or 4 swipe commands based on user card programming to initiate a different sequence of events depending on the need.
- 1.21. The controller panel shall be capable of storing up to eight (25) custom card/tagcard/tag/tag formats and reading 5 formats simultaneously. The controller panel shall be able to read the format of most Magnetic Stripe, Bar Code, Proximity or Wiegand Effect encoded card/tagcard/tag/tags and shall allow an operator to specify parity, start sentinels, stop sentinels, field separators, facility code bits, issue level bits, and card/tagcard/tag/tag number bits.
- 1.22. The controller panel shall be capable of reading card/tag numbers up to eighteen (18) digits.
- 1.23. The controller panel shall have the capacity to store up to 128 time zones with each time zone consisting of up to 16 intervals of time. Each interval of time shall consist of a range of days (seven days of the week, in addition to a Holiday Schedule) as well as a range of time. The controller panel shall automatically manage time zones based upon its internal clock.
- 1.24. The controller panel shall allow for the definition of up to 365 Holidays. Holidays shall be defined according to day of year and time of day. All holidays shall be automatically incorporated into Time Zone definitions.
- 1.25. Each card/tag reader/keypad shall have the ability to independently operate in up to six different modes: Card/tag reader only, PIN only, Common Code only, Card/tag Reader plus PIN, High Security and Free Access. These modes of operation shall be programmed from the system host computer and shall automatically change by time zone assignment.
- 1.26. The system shall support interlock groups for Man –trap operation.

- 1.27. The controller panel shall allow for the support of anti-passback operation, in which card/tagholders must follow a proper in/out sequence.

UNC100 CONTROLLER

- 1.28. The controller panel shall be a 32 bit microprocessor controlled solid-state electronic device and shall include a real time clock/calendar on board. Boards shall be made of gold-plated construction (Copper or leaded will not be accepted) and incorporate flashware technology. Communication shall One channel TCP/IP standard LAN/WAN windows environment protocol. A subset of the system database sufficient to support access and alarm functions for its designated readers and points shall be stored at the controller panel. In event of communication loss, the controller panel shall continue to function without degradation of operation and shall provide storage of a least 10,000 events. These stored events shall be uploaded to the CPU automatically upon restoration of the communications. The system shall be capable of performing all system functions indefinitely without the computer.
- 1.29. The controller must be FCC, CE, RoHS and UL listed.
- 1.30. The controller must have 2mb Ram available on board
- 1.31. The controller must have 50,000 offline event buffer
- 1.32. The controller must have 1 programmable RS485 ports
- 1.33. The controller must have 2 on board Wiegand reader ports to accept any Wiegand format and 5 Wiegand formats simultaneously.
- 1.34. The controller must have 4 fully supervised inputs capable of individual configuration for EOL (single and dual EOL), N.O, N.C. operation.
- 1.35. The controller must have 4 outputs. 2-form 'C' relay outputs rated at 10A-30VDC and 2-open collector 100ma outputs.
- 1.36. The Controller must have separate tamper input
- 1.37. Input voltage 12vdc or 30w P.O.E. maximum current draw 500ma
- 1.38. The controller must have internal charging circuit for 12vdc gel cell standby battery. The controller shall be capable of recharging a standby battery from either P.O.E. source or 12v local power supply.
- 1.39. The controller shall be configurable in the following methods. Edge device, Wall mount controller.
- 1.40. Edge device deployment shall be POE and operate continuously even if POE is lost. Edge controller shall operate 1 or 2 doors as desired.

- 1.41. The controller must accept and control up to 7 slave reader controllers and 16 I/O controllers simultaneously.

RBH-IOC-16 Input Output Controller

- 1.42. Additional inputs and outputs shall be available by adding IO boards. Each expansion board shall have a minimum of sixteen (16) supervised inputs or outputs. The inputs shall incorporate full supervision of 7 circuit types and the outputs shall be form "C". Up to sixteen (16) expansion boards shall be available for each controller panel.
- 1.43. The IO board shall be independently powered and have its own back up power supply and charging circuit for a minimum 4 hour standby operation.

RBH- ENCL2 Wall Cabinets

- 1.44. The controller panel enclosure shall have a hinged cover with key lock. A control panel input point shall monitor an enclosure tamper switch.
- 1.45. The cabinet shall be 22" X 18" X 4" with ½ and ¾ inch knockouts. The back of the cabinet shall have key mounts for easy mounting.
- 1.46. The cabinet shall hold any two of the following controllers UNC500, NC100, RC2, IOC16

NC100 Controller Panel Firmware Features

- 1.47. The controller panel shall have the ability to store up to 7000 card/tagcard/tag/tag/pin codes expandable to 500,000 and buffer up to 10,000 transactions expandable to 500,000.

CARD/TAG READERS & CARD/TAGS

- 1.48. The system shall employ a proximity access control/identification technology that utilizes radio frequency (RF) circuits in microchip form. The microchips are encoded and transmit the encoded information when activated.
- 1.49. The readers shall be any weigand output or equivalent proximity/iclass/mifare type. It shall read the identification number of the card/tag or tag when presented to the surface of the reader without physical contact.
- 1.50. Single piece window/door frame reader, which shall mount directly on a standard 1.75" (4.5cm) metal mullion/door frame. The reader can be mounted indoors or outdoors on virtually any surface, including metal. The reader shall operate between 5 volts and 14 volts DC to allow for ease and flexibility in installation. Read range with a standard proximity card/tag shall be up to 4" (up to 10cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader shall be 5.5" (14.0cm) High x 1.6" (4.1cm) Wide x 0.75" (1.9cm) Thick.
- 1.51. A single piece wall switch reader, which shall mount directly on a standard metal or plastic single-gang electrical box, or on a flat wall or metal surface, and shall operate indoors or outdoors. The reader shall operate between 5 volts and 14 volts DC to allow for ease and

flexibility in installation. Read range with a standard proximity card/tag shall be up to 4" (10cm) when installed according to the manufacturer's specifications. Maximum dimensions of the reader shall be 4.6" (11.7cm) High x 2.9" (7.6cm) wide x 0.5" (1.3cm) Thick.

- 1.52. A single piece reader, which shall mount to any surface, including metal, or can be concealed behind most building materials, except metal. Read range with a standard proximity card/tag shall be up to 7" (17cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader shall be 4.6" (11.7cm) High x 5.5" (14cm) Wide x 1.4" (3.6cm) Thick.
- 1.53. A medium range reader, which shall mount to most surfaces, except directly on metal, or can be concealed behind most building materials, except metal. Read range with a standard proximity card/tag shall be up to 21" (42cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader head shall be 8.8" (22.4cm) High x 8.8" (22.4cm) Wide x 1.14" (2.9cm) Thick.
- 1.54. The card/tag or tag shall be read when presented in any orientation or at any angle to the surface of the reader within the proper read range
- 1.55. The reader shall power the card/tag or tag, process the encoded data, and output the data to the access system in less than 110 milliseconds.
- 1.56. There shall be no removable plate or cover, which allows access to the reader electronics.
- 1.57. A red/green LED on the front surface of the reader shall indicate to the user that the card/tag or tag was read (internal/reader controlled) and an access decision was made (system controlled). The LED may be configured in either single line mode or dual line mode (allowing an "off" state) as required by the host system, and the reader may be switched between modes by presenting a programming card/tag to the face of the reader.
- 1.58. The reader shall have an audio "beep" tone feature to indicate to the user that the card/tag or tag was read (internal/reader controlled) and an access decision was made (system controlled). The audio tone must be independently controllable and not tied to the status or colour of the LED. The internal control of the LED and beeper may be enabled/disabled via programming card/tags so as not to require the setting of switches internal to the reader.
- 1.59. The reader shall have a built-in diagnostics, which indicate to the installer that upon power up the reader has performed an internal test and is functioning properly.
- 1.60. The reader shall have a built-in diagnostic feature, which allows a single technician to test the continuity of the data lines independent of the door controller. The reader may be placed into the line diagnostic mode via a programming card/tag, and the technician can then measure the pulses at the end of the line without the need of a second technician at the reader presenting card/tags.
- 1.61. Electrical connections between the reader and the controller shall be via colour coded, multiconductor; #22 AWG shielded cable. No coaxial cable or special connectors shall be required. The output shall be in the form of Wiegand data stream.

- 1.62. Wiring from the reader assembly to the system interface or CPU shall be run inside metal conduit or EMT, as may be required by electrical codes. All junction boxes are to be concealed and bot normally accessible to the public. Utilization of PVC conduit is not acceptable.
- 1.63. Accidental or intentional transmission of radio frequency signals into the reader shall not compromise the system.
- 1.64. The reader shall function in the access control system's normal or anti-passback mode without changes to the reader.
- 1.65. The reader operating temperature range shall be -40° to +50° C
- 1.66. Damage or vandalism to the reader shall not damage any other part of the system.
- 1.67. Tampering with the reader shall have no effect on the door security.
- 1.68. The system readers shall have the capability to accept codes from any of the following proximity devices:
 - 1.69. A standard molded plastic credit card/tag sized card/tag having maximum dimensions of 3.41" (8.7cm) x 2.14" (5.4cm) x 0.09" (0.23cm), and a weight of not more than 0.48 oz. (13.5g). A punched slot shall be provided for a strap or clip. The card/tag shall be capable of having multi-colour custom graphics and permanently marked numbers printed directly onto both sides.
 - 1.70. A tag having maximum dimensions of 2.2" (5.6cm) x 1.3" (3.3cm) x 0.25" (0.6cm), and weight of 0.36 oz. (9.9g). A brass eyelet shall be provided for attachment to a key ring.
 - 1.71. A credit card/tag sized card/tag made of PVC, having maximum thickness of .036", and the capability of accepting direct print video imaged graphics and photographs and able to carry a high coercivity magnetic stripe.
 - 1.72. A credit card/tag sized card/tag having maximum thickness of .048", and capable of accepting a photograph and graphics via a customer laminated flap.
 - 1.73. The card/tag shall be a polycarbonate-based card/tag that cannot be run through direct card/tag printers. The card/tag shall be a PVC dual technology card/tag that employs proximity sensor technology. It shall comply with ISO standards for thickness (30 mil).
 - 1.74. The card/tag or tag shall be made of robust ABS plastic to provide maximum protection for the circuitry inside and provide minimal flexing which could cause damage to the card/tag.
 - 1.75. The presence of small metal objects, such as keys or coins near the card/tag or tag shall not alter the code read by the reader, nor prevent the code from being read by the reader.
 - 1.76. The card/tag shall be of a proprietary format to be controlled by the Owner.
 - 1.77. Card/tags or tags shall be sequentially numbered. The user may specify codes or numbers.

- 1.78. The card/tag must have the ability to have the encoded number permanently marked on the outside surface.
- 1.79. The card/tag or tag shall be a passive device with no internal battery, but shall contain a semiconductor element, which is energized when brought within the operating range of the reader causing transmission of the code from the card/tag or tag to the reader. Card/tags requiring an internal battery or energy cell shall not be acceptable.
- 1.80. Card/tags and tags may be used interchangeably and shall be compatible with all readers in the system, regardless of the reader's physical size or style, and without any code matching or memory devices in the reader.
- 1.81. The card/tag and tag operating temperature range shall be -40° to +50° C

2. Fingerprint/Biometric Readers and Software Integration

- 2.1. The fingerprint reader shall be RBH-BFR.
- 2.2. The software shall have an integrated tab in the cardholder screen to enable the operator to enroll fingerprints/ biometrics directly from the software. Programs that open third party software are unacceptable.
- 2.3. The capture template will allow the capture of a primary and secondary finger as a backup.
- 2.4. The authentication will be automatically downloaded to the reader upon successful capture of the fingerprint without intervention by the operator. The download shall be by TCP/IP communications to the fingerprint readers.
- 2.5. The fingerprint must be saved as an algorithm to protect individual privacy.
- 2.6. The fingerprint algorithm shall be saved within the normal AxiomV database for automatic backup and restore capabilities. External backup systems for fingerprint are not acceptable.
- 2.7. The fingerprint reader shall be configurable to operate in any of the following modes. Finger only, Card only, card plus finger, Finger plus PIN code, Finger or Card.
- 2.8. The reader shall have a Wiegand output to connect to the door control panel

3. ACS VMS INTEGRATION

- 3.1. Integration must be through TCP/IP (relay and or RS232 connections are not acceptable).
- 3.2. All devices within the ACS system must have a tab to associate a video camera from the VMS system to the device. This association must allow the camera to be called into the ACS GUI upon the following conditions. A) Any Incoming event from specified device B) Any incoming alarm from the specified device. The camera if PTZ must also be called to its predesignation preposition.
- 3.3. The ACS must be able to connect to the VMS system and display the VMS's default video window as a native VMS viewing client.

- 3.4. The ACS must have the ability to pop-up any video event designated for pop-up without operator intervention.
- 3.5. The ACS must have the ability to manually call video by clicking on the event anywhere it appears in the ACS.
- 3.6. The ACS must have the ability to dynamically place the cameras from the VMS system on its maps and call video from the maps directly.
- 3.7. The ACS must have the ability to report all events tagged with video and play back directly from the report within the ACS GUI.

ALARM KEYPADS

The system shall incorporate alarm keypads that link directly to the system for advanced alarm operation. Operators can arm, disarm, send messages and monitor any alarm on the keypad. In addition the keypads shall have entry exit zones and the ability to initiate commands on the system by entering a code or command. The keypads will have the ability to arm or disarm any group of inputs on the system creating a seamless alarm intrusion panel.

ALARM MONITORING INTEGRATION

- 3.8. The system shall allow for annunciation of intrusion detection alarms. Intrusion detection alarms shall report just like any other access control alarm and shall have the same annunciation and display properties as access control alarms.
- 3.9. Alarms from the alarm keypad shall be displayed in the alarm monitoring window and any signal can be sent out via TCP/IP or message port.
- 3.10. The system shall support an Alarm Details description that shall show the 'Alarm Description', 'Time/date', 'Controller', 'Device', and 'Area' associated with the alarm. The information shall also display the user.
- 3.11. The system shall support tracing of intrusion detection devices and areas.
- 3.12. The system shall be able to report status information for the intrusion detection devices.
- 3.13. On alarm, the system shall automatically switch to the map that displays the alarm, the icon that represents that alarm point will flash and an audible alert will be generated on the computer sound system. The operator shall have to acknowledge the alarm before processing the alarm.
- 3.14. In operator alarm mode processing, the system shall allow the operator to:
 - 3.14.1. clear alarm, tamper, and diagnostic alarms

- 3.14.2. observe CCTV camera views, individually or in groups, that are associated with an alarm (requires video switcher option)
- 3.15. In operator normal mode processing, the system shall allow an operator to:
 - 3.15.1. view a list of activity information, and select and tag any event
 - 3.15.2. view site maps
 - 3.15.3. perform a test of testable devices/sensors
 - 3.15.4. change the state of sensors to access or secure
 - 3.15.5. review the last 1000 events/actions performed on the system
- 3.16. In maintenance processing, the system shall allow the maintenance technician to:
 - 3.16.1. assign passwords and function access to individual users
 - 3.16.2. examine the input/output point states
 - 3.16.3. adjust the sensitivity of the sensors
 - 3.16.4. access the operating system to diagnose system problems
 - 3.16.5. set the calendar clock's date and time (in Windows)
 - 3.16.6. change the format of the displayed date (in Windows)
 - 3.16.7. set the communication parameters for system devices
 - 3.16.8. shut down the system

WIRELESS LOCKSET INTEGRATION

The system shall support the integration of SALTO SALLIS wireless locksets with the security management system.

The wireless system and components shall offer as a minimum:

- 3.17. Wireless Radio Frequency based on IEEE 802.15.4 at 2.4 GHz.
- 3.18. Wireless communication shall incorporate AES 128bits encryption.
- 3.19. Reading time shall be less than 150 milliseconds.
- 3.20. Card reader ID technologies for the locks shall be able to read one of these: Mifare, Mifare plus, DESfire, DESfire EV1, HID iClass.

- 3.21. Powering by standard non-proprietary, commercially available batteries. Renewal of batteries shall only be permissible from the secure side of any door with access to the battery compartment only achievable by the use of non-commercially available tool sets provided exclusively by the manufacturer.
- 3.22. All electronic locking devices must be able to be temporarily activated by an appropriate device in the event of total battery failure.
- 3.23. The access control system shall have a comprehensive battery management reporting system to allow for the viewing of the battery status of any locking device in the system at any time.
- 3.24. The locking devices themselves shall provide, upon activation by a credential or other means, a distinguishable and audible signal when any battery is reduced to its last 1,000 usable cycles.
- 3.25. The system shall support more than 500 remote locksets; each UNC100 controller configuration shall be rated for the number of locksets it can support.
- 3.26. Once a lockset is installed and registered with the controller, it shall appear in the AxiomV software as a traditional access point, which can be enabled and configured to work with the controller.
- 3.27. When a wireless lockset is networked to the AxiomV software, the operator shall be able to lock or unlock in real-time, the lock, under 2 seconds.
- 3.28. All locksets connected to the AxiomV software shall be treated as an online lockset and assigned the Default (Online) lockset profile.
- 3.29. Locksets can be assigned to locations.
- 3.30. Locksets shall be added and managed in floorplans.
- 3.31. Locksets can be unlocked momentarily via event actions or from the AxiomV client, the AxiomV mobile app, the Monitoring Desktop, or a floorplan within one minute.
- 3.32. Activity associated with a lockset shall be viewed in real time in the Activity Log.

Installation

- 3.33. The contractor shall install all system components in accordance with the manufacturer's instructions, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. Power, control, signal and communications, and data transmission lines plus all required grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation. Provide mounting hardware as required.
- 3.34. All products, software, programming tools, etc. shall be registered to The Owner and will be surrendered upon successful completion of the project.

- 3.35. All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code. Cable shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring.
- 3.36. All inputs shall be protected against surges induced on device wiring. Outputs shall be protected against surges induced on control and device wiring installed outdoors. All communications equipment shall be protected against surges induced on any communications circuit. All cables and conductors, except fibre optics, which serve as communications circuits from security console to field equipment, and between field equipment, shall have surge protection circuits installed at each end.
- 3.37. No wiring or cabling shall be exposed; all wiring and cabling must be fully enclosed in threaded metallic conduit, which shall be installed underground, in walls or metal structures unless physically impossible. Any conduit that is exposed shall be fully enclosed within an expanded metal protective cage that is vandal resistant and is equipped with a tamper alarm. All equipment mounting is to be such that the equipment cannot be removed or tampered.

CARD READERS

The access control shall only utilize readers supplied HID Global. The readers will support multi card formats and be available in multiple form factors and transmit power ratings.

- 4.1 Support for iClass, iClass Seos, MIFARE Classic, MIFARE DESFIRE EV1 @ 13.56 MHz transmit frequency.
- 4.2 Support for HID Prox, Indala Prox, EM4102 Prox at 125 KHz transmit frequency.
- 4.3 Support an operating voltage range of 5-16 VDC.
- 4.4 Support OSDP SC over RS485 for panel communications and reader firmware updates.
- 4.5 Support an operating temperature range -35° C to +65° C.
- 4.6 Support a storage temperature range of -35° C to +65° C.
- 4.7 Support an operating humidity range of 5% to 95% relative humidity.
- 4.8 Carry an IEEE IP55 rating, IP65 with optional gasket, part #IP65GSKT.
- 4.9 Carry the following industry certifications: UL294/cUL and Industry Canada.
- 4.10 Carry a limited lifetime warranty.

END OF SECTION

28 23 00 Video Surveillance

VMS Applications

The enterprise VMS software installed at City of Brampton sites are to be manufactured by March Networks. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.4 of this document.

PART 1 GENERAL

1.1 SECTION INCLUDES

- A. Command Enterprise Server Software

1.2 RELATED SECTIONS

- A. Section 26 05 00 - Common Work Results for Electrical
- B. Section 27 11 23 - Communications Cable Management and Ladder Rack

1.3 REFERENCES

- A. Canadian ICES-003.
- B. Consultative Committee for International Radio (CCIR).
- C. Conformity for Europe (CE).
- D. Electronic Industry Association (EIA).
- E. Federal Communications Commission (FCC).
- F. Joint Photographic Experts Group (JPEG).
- G. National Television Systems Committee (NTSC).
- H. Phase Alternating Line (PAL).
- I. Underwriters Laboratories Inc. (UL).

1.4 DEFINITIONS

- A. HD (High-definition) - refers to video having resolution substantially higher than traditional television systems. HD has one or two million pixels per frame.
- B. CIF (Common Intermediate Format) - refers to a standard video format, which is categorized based on the resolution.

1.5 SUBMITTALS

- A. Manufacturer's Product Data: Submit manufacturer's data sheets indicating systems and

components proposed for use, including instruction manuals.

- B. Operation and Maintenance Data: Submit manufacturer's operation and maintenance data, customized to the system installed. Include system and operator manuals.

1.6 QUALITY ASSURANCE

- A. Manufacturer shall provide customer service, pre-sales applications assistance, after-sales technical assistance, access to online technical support, and online training using Web conferencing.
- B. Manufacturer shall provide 24/7 technical assistance and support by means of a toll-free telephone number at no extra charge.
- C. Installer: Minimum two years' experience installing similar systems, and acceptable to the manufacturer of the video management system.
- D. Power Requirements: Components shall have the following electrical specifications: 100-240 V AC (50 Hz/60 Hz) or as specified for individual products within part 2 of the specification.

1.7 DELIVERY, STORAGE, AND HANDLING

- A. Deliver and store products in manufacturer's unopened packaging bearing the brand name and manufacturer's identification until ready for installation.
- B. Handling: Handle materials to avoid damage.

1.8 PROJECT CONDITIONS

- A. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results. Do not install products under environmental conditions outside manufacturer's recommended limits.

1.9 SEQUENCING

- A. Ensure that products of this section are supplied to affected trades in time to prevent interruption of construction progress.

PART 2 PRODUCT

2.1 MANUFACTURER

Acceptable Manufacturer: March Networks, which is located at: 303 Terry Fox Drive, Suite 200; Ottawa, Ontario, Canada K2K 3J1; Toll Free Tel: 800-563-5564; Email:sales@marchnetworks.com; Web:www.marchnetworks.com

2.2 COMMAND ENTERPRISE SERVER SOFTWARE

- A. System Software Characteristics

1. The Enterprise server software shall run on a stand-alone or virtualized server, separate from any recording server software.
2. The Enterprise server software database server shall contain a database of all network-connected recorders, recording servers, edge devices and their configurations. The database shall contain details including:
 - i. System configuration
 - ii. Camera configuration and settings
 - iii. Recorder configuration and settings
 - iv. System users
 - v. Health parameters
 - vi. Alarm parameters
3. An Enterprise server software database shall be included with the primary installation package and shall not require the customer to install a separate installation of the database.
4. The Enterprise server software database shall be independent to allow customers to install their system on their existing SQL database environment within the limitations of the Enterprise System Software supported database characteristics.
5. The system independence shall allow host/storage platforms to be supplied optionally by the Enterprise software manufacturer, the system integrator or the customer IT.
6. The Enterprise server software shall support enterprise grade virtualization.

B. Network Communications

The Enterprise solution shall have robust IP networking features, in line with IT management team expectations. These features shall include the following:

1. Servers running the Enterprise software shall connect to an enterprise LAN or WAN network via a Gigabit Ethernet connection. The client viewing and configuration applications shall operate on workstations connected (locally or remotely) to the LAN/WAN using network connections to support the number of desired cameras viewed per workstation, and shall communicate with the VMS across this network. The Enterprise system host server(s) and client applications shall communicate using the TCP/IP protocol.
2. The Enterprise Server software shall operate using either DHCP or static IP addressing. If using DHCP addressing, client software must be able to connect to an Enterprise server using its new address without any action on the part of the user.
3. The Enterprise solution shall operate using a peer-to-peer architecture with no central video-streaming server and there shall be no imposed limit to the scalability of the system.
4. The Enterprise Server software shall require HTTP and HTTPS connections for communications.

C. Enterprise Server Software

At the core of the IP video solution, the Enterprise Server software shall have the following characteristics:

1. The Enterprise server software shall be host-hardware-independent and be purpose-built for the system management.
2. The Enterprise server software shall be compatible with any of Windows® Server 2012 and 2012 R2, Windows® Server 2016 and Windows® Server 2019 operating systems.
3. The Enterprise server software shall support LDAP/Microsoft Active Directory for user authentication.
4. The Enterprise server software shall not reside on the same server as the LDAP/Microsoft Active Directory Server component.
5. The Enterprise server software shall run Oracle Glassfish Enterprise Server.
6. The Enterprise server software shall run a SQL database engine from a top manufacturer such as Microsoft, Oracle or others.

D. General

The primary client software shall support an integrated license management, user management and system health monitoring applet with the following characteristics:

1. This shall be an enterprise-class central management utility, addressing all related software license management and user access privileges management. It shall also provide comprehensive, real-time system health maintenance functions. These capabilities shall extend seamlessly across any number of video installations and any number of network-linked physical locations. All local and remote management functions shall operate over a TCP/IP LAN or WAN network.
2. This utility shall consist of the user interface within the client interface and a necessary server-based software engine. Together these software components shall provide the management functionality described in this Section.

E. Licensing

The Enterprise server software manufacturer shall license the software per manufactures Hybrid/NVR recorders on a per video channel basis for manufacturers VMS recorders, in such a way that there are no license fees associated with client applications, site installation, user accounts, basic add-on features or other license fees. The licensing program characteristics are:

1. The enterprise system shall have an enterprise base license that allows access to all basic features and functionalities without any additional licenses except camera licenses.
2. Edge device license shall not be tied to a hardware address (MAC Address).
3. The Enterprise Server software shall not be tied to the server hardware.
4. Camera licenses may be moved between recording servers.
5. All camera licenses are moveable without requiring manufacturer action of any type.

6. The enterprise system shall include 10,000 recorder connection licenses.
7. All embedded recorder licenses include all channels of video associated with the recorder whether the unit is a 4, 8, 12, 16, 24, 32, 48, or 64 channel unit. No additional edge device licenses are needed when a recorder has a valid connection license.
8. Each VMS recorder server shall be capable of supporting 128 edge device connection licenses.
9. All basic VMS client software shall be included in the base VMS software cost.
10. The client application can be used on an unlimited number of times and may be running simultaneously without any additional licenses.
11. The enterprise system software base license shall be capable of supporting 10,000 recording servers/recorders licenses and/or 128,000 edge device connection licenses.
12. The enterprise system shall support the ability to license additional components such as third party access control integration plugins, video or sensor analytic channels, and other manufacturer's applications that sit on top of the enterprise system.

F. Administration Functionality

The client shall provide the user interface for the licensing, user management and system health management activities introduced above. It shall be accessed by authorized users from within the primary client application and its features and functions shall include but not be limited to the following:

1. Software License Keys shall be the technology used to officially enable Enterprise capacities and capabilities, including enterprise server licenses, edge device connections, NVR connections, DVR connections, enhanced applications, etc. The client shall provide the mechanism for entering, activating, updating and tracking the status of all related licenses in a single or multi-server environment.
2. The software shall provide enhanced user access control, including matching authorized system administrators to individual or groups of recording servers/recorders and allowing them to review, modify and update programming remotely.
3. The software shall be used to manage access privileges for all other system users as well. Authorized Administrators shall be able to define user names, passwords and access rights, as well as logical groupings recording servers, recorders, views, and individual users. Users shall be assigned to groups which have defined privileges, and these groups shall be assigned access to the appropriate system resources.
4. Privilege management shall provide a specific level of granularity, allowing access to be controlled down to logical groups of resources including cameras, recorders, views, maps, and logical folders.
5. The client shall include a complete set of features for monitoring the health of the complete video surveillance infrastructure, including all local and remote recorders/recording servers, storage devices and hard drives, IP cameras, encoders and any other solution elements.

6. Health alert triggers shall include but not be limited to failed network connections, unit performance problems, camera synchronization loss, recording server temperature exceptions, and more for select recording solutions.
7. Health alert triggers shall support thresholds to limit the number of alerts visualized and stored by the enterprise system. Thresholds shall support the ability to filter issues by number of occurrences per type, number of occurrences in time, and a combination of the above.
8. The Enterprise system shall automatically and without user intervention provide a process whereby critical system events including alarms shall be visually brought to the attention of the user.
9. The Enterprise system shall visually notify the user if a server becomes unreachable during a session.
10. The Enterprise system client shall be capable of monitoring a recording servers/recorders and reporting the following items:
 - a. Installed recording software version.
 - b. Total amount of system memory.
 - c. Total amount of available system memory.
 - d. Total CPU utilization.
 - e. Video source status including current recording status.
 - f. Provide a list of events that have occurred on the selected server since the initial connection.
11. Listing of currently connected clients including connection number, client (source) IP address, description of the client and the username used by the selected client
12. The Enterprise system shall support “single seat administration” so that a single management application administers multi-server/multi-client environments. This allows simultaneous control of multiple servers and clients and system-wide monitoring of the health and status of all recording servers/recorders and cameras from one console. Support is included for:
 - a. Push-based, secure, distribution of application configuration for all VMS recording server software components where the update process occurs in parallel for all selected servers.
 - b. Pull-based configuration updates of recorders/recording servers, and edge devices.
 - c. Support for remote configuration of all VMS recording server/hybrid servers in the enterprise network.
 - d. Support for remote monitoring of all VMS recorder/recording server software components.
 - e. Manage recorder and device licenses centrally
 - f. Centrally configure users
 - g. Centrally configure logical folders, add/remove resources from folders.
 - h. Replicate users
 - i. Replicate device configuration across like kind device types and recorders.

G. Resource Detection and Configuration

1. The Enterprise Server software shall have the ability to register/unregister physical recording server, hybrid NVR and NVR recorders.
2. The Enterprise Server software shall offer the ability to auto-discovery all recording servers and hybrid network video recorders in the Enterprise Server LAN and associated edge devices in the managed video surveillance network.
3. The Enterprise Server shall be able to initiate a proxy session to any IP edge device with a recorder. The Enterprise Server client shall be able to launch a session with the cameras page if the platform allows it.

H. Mass Management

1. The server software shall host the database for maintaining select manufacturer's edge device configurations and firmware status.
2. The server software shall support secure connections, registration, and the ability to send configuration changes to recording servers and hybrid network video recorders.
3. The server software shall support the ability to import device configurations and have the ability to send device configuration upon request.
4. The server software shall support the ability to import a devices full configuration, and export the full configuration to one or many manufacturer's edge devices on the network.
5. The server software shall have the ability to import/export the manufacturer's edge devices configuration details including:
 - a. Frame rate
 - b. Resolution
 - c. Compression algorithm
6. The server software shall have the ability to accept current configurations from select edge devices from IP cameras and encoders developed by the manufacturer.
7. The server software shall allow for mass configuration of recorders, recording servers, and edge devices. This shall include the ability to do the following:
 - a. Copy Configuration
 - b. Apply Configuration
 - c. Monitor Configuration
 - d. Associate Configuration
 - e. Update Configuration

I. Firmware Management

1. The server software shall allow the ability to apply firmware from the enterprise server to one or many edge devices manufactured by the manufacturer at a single time.

2. The server software shall allow the ability to apply firmware from the enterprise server to one or many recorders manufactured by the manufacturer at a single time.
3. The server software shall allow the ability to limit the number of concurrent firmware updates and the total recorders incoming bandwidth and enterprise system outgoing bandwidth used for the updates.
4. The server software shall allow the ability to store the most current device firmware on the enterprise server.
5. The enterprise server shall provide a visual notification when any one device is not current with the most current version of firmware on that is available on the enterprise server.
6. The server software shall support the ability conduct the following actions for edge devices firmware management.
 - a. Upload firmware
 - b. Apply firmware
 - c. Restore firmware

J. System Security and Reliability

The Enterprise Server software shall provide the following system-wide IT defenses and security capabilities view:

1. Each Enterprise host server shall be capable of being deployed 'behind' a standard and likely existing LAN/WAN security firewall, benefiting from the virus and malware protection software and other encryption and intrusion defenses in place on that network.
2. The Enterprise system shall minimize the number of access points attackers could attempt to exploit to gain access to the system or at which a virus or similar form of malicious software may be directed to compromise the operation of or the data associated with the system. All communication with the Enterprise system shall be tightly restricted, with most external communication ports being permanently blocked from user access (and with no way made available to open them). This includes all TCP and UDP ports not required for system operation.
3. All analog video shall be captured, digitized and transmitted over the secure network to the VMS using encoders. Analog video shall be streamed to these encoders over coaxial cables connected directly to these devices. No interception of these video streams shall be possible without physically tapping into the specific cables inside the customer premises.
4. All IP-camera video shall be captured and transmitted to the VMS over the secure network using the IP protocol.
5. The VMS shall support multiple levels of user and administrator password authentication and privileges management to control access to the system. A fully configurable matrix of user accounts, user groups and user privileges shall be supported. In an enterprise configuration, user authentication through a corporate application (i.e., Windows® Domain Server) shall also be supported via the Enterprise

server. The result shall be a single authentication functionality via this existing IT access management utility.

6. User authentication shall support the use of optional identification certificates on smart cards or USB tokens in conjunction with user credential authentication.
7. User and administrator access rights shall be fully configurable, down to the individual video resource level (i.e., to a specific camera). These rights shall apply to local and remote users equally.
8. Each VMS shall keep a running log of all user access. These logs shall be retrievable by authorized administrators, but no user shall be able to remove entries from a log. It shall be an option to copy and save a log in a text-formatted file appropriate for printing. This text file shall also be suitable for import into a third-party report management application.
9. The VMS shall contain software watchdog technology that maximizes fault-free operation. The central management application shall continuously monitor the health of the servers, edge devices, cameras and the network. It shall automatically report all problems detected per preset notification policies.
10. The Enterprise Management Software provider shall provide publicly available information on their website that lists known Security Vulnerabilities with software release versions required to address the vulnerability.

PART 3 EXECUTION

3.1 INSTALLATION

- A. All components of the video management system shall be thoroughly tested before shipping to the project location.
- B. Video management system shall be installed, programmed and tested in accordance with manufacturer's installation instructions. The integrator shall:

Coordinate interfaces with Owner's representative where appropriate.

Provide backboxes, racks, connectors, supports, conduit, cable, and wire for a complete and reliable installation. Obtain Owner's approval for exact location of all boxes, conduit, and wiring runs prior to installation.

Install conduit, cable, and wire parallel and square with building lines, including raised floors areas. Do not exceed forty percent (40 percent) fill in conduits. Gather wires and tie to create an orderly installation.

Coordinate with other trades to provide proper sequencing of installation.

3.2 FIELD COMMISSIONING

- A. Test video management system as recommended by manufacturer, including the following:

1. Conduct complete inspection and testing of equipment, including verification of operation with connected equipment.
2. Test devices and demonstrate operational features for Owner's representative and authorities having jurisdiction, as applicable.
3. Correct deficiencies until satisfactory results are obtained.
4. Submit written copies of test results.

3.4 TRAINING AND CERTIFICATION

- A. The Enterprise Management software manufacturer shall offer free online training for authorized dealer technicians through user controlled portal access.
- B. Training material shall cover all aspects of installation, configuration and maintenance.
- C. The dealer shall receive a certificate upon the successful completion of the certification exam. Certifications shall be valid for a period of 2 years.
- D. The Enterprise Management software manufacturer shall offer free online training tutorials for system administrators accessible 24/7 via open (non-restricted) website for an unlimited number of system users. The training tutorial shall cover the Enterprise system, User management, Health alert management and Mass Management (upgrades) of all registered devices on the Enterprise Server.
- E. The Enterprise Management software manufacturer shall offer free online training for Guards and Investigators accessible 24/7 via open (non-restricted) website for an unlimited number of system users. The training tutorial shall cover system access, live and archive media requests, alarm inbox management, as well as extracting media from the system

END OF SECTION

Network Video Recorders

PART 1 GENERAL

The network video recorders installed at City of Brampton sites are to be manufactured by March Networks. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.4 of this document.

1.1 SECTION INCLUDES

- B. 8000 Series Hybrid Network Video Recorders

1.2 RELATED SECTIONS

- C. Section 26 05 00 - Common Work Results for Electrical
- D. Section 27 11 23 - Communications Cable Management and Ladder Rack

1.3 REFERENCES

- A. Canadian ICES-003.
- B. Consultative Committee for International Radio (CCIR).
- C. Conformity for Europe (CE).
- D. Electronic Industry Association (EIA).
- E. Federal Communications Commission (FCC).
- F. Joint Photographic Experts Group (JPEG).
- G. National Television Systems Committee (NTSC).
- H. Phase Alternating Line (PAL).
- I. Underwriters Laboratories Inc. (UL).
- J. Regulatory
 - a. The recorder shall have passed the following safety standards:
 - IEC60950-1 (ed.2)
 - UL 60950-1 (ed.2)
 - CSA C22.2 No.60950-1-07 (ed.2)
 - b. The recorder shall conform to the following FCC rules and regulations:

- EMC FCC 47 CFR Part 15 (Subpart 15)
 - ICES-003
 - EN55022, CISPR 22, AS/NZS CISPR 22
 - EN61000-3-2, EN 61000-3-3
 - EN50130-4, EN55024
- c. The recorder shall have the following markings indicating compliance with the regulations for sale into the countries that accept the marking:
- CE-mark
 - cULus
 - C-tick
 - WEEE

1.4 DEFINITIONS

- A. HD (High-definition) - refers to video having resolution substantially higher than traditional television systems. HD has one or two million pixels per frame.
- B. CIF (Common Intermediate Format) - refers to a standard video format, which is categorized based on the resolution.

1.5 SUBMITTALS

- A. Operation and Maintenance Data: Submit manufacturer's operation and maintenance data, customized to the system installed. Include system and operator manuals.
- B. Field Tests: Submit results of field testing of every device including date, testing personnel, retesting date (if applicable), and confirmation that every device passed field testing.

1.6 QUALITY ASSURANCE

- A. Manufacturer shall provide customer service, pre-sales applications assistance, after-sales technical assistance, access to online technical support, and online training using Web conferencing.
- C. Manufacturer shall provide 24/7 technical assistance and support by means of a toll-free telephone number at no extra charge within the terms of the warranty agreement.
- D. Installer: Minimum two years' experience installing similar systems, and acceptable to the manufacturer of the video management system.
- E. Power Requirements: Components shall have the following electrical specifications: 100-240 V AC (50 Hz/60 Hz) or as specified for individual products within part 2 of the specification.

1.7 DELIVERY, STORAGE, AND HANDLING

- A. Deliver and store products in manufacturer's unopened packaging bearing the brand name and manufacturer's identification until ready for installation.

- B. Handling: Handle materials to avoid damage.

1.8 PROJECT CONDITIONS

- A. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results. Do not install products under environmental conditions outside manufacturer's recommended limits.

1.9 SEQUENCING

- A. Ensure that products of this section are supplied to affected trades in time to prevent interruption of construction progress.

1.10 WARRANTY

- A. The recorder shall have a warranty of at least 3 years.
- B. Should the recorder fail during the warranty period, a replacement recorder shall be available as an advance replacement at no additional cost in order to return the end user to full functionality as quickly as possible.

PART 2 PRODUCT

2.1 MANUFACTURER

Acceptable Manufacturer: March Networks, which is located at: 303 Terry Fox Drive, Suite 200; Ottawa, Ontario, Canada K2K 3J1; Toll Free Tel: 800-563-5564; Email:sales@marchnetworks.com; Web:www.marchnetworks.com

2.2 8000 SERIES HYBRIDE NETWORK VIDEO RECORDERS

- A. Recorder Characteristics – Combined with visual intelligence software, the NVR unit shall have the following characteristics:
 - 1. The system shall be a networked device purpose built exclusively for the capture and processing of digital video and supporting audio, metadata, alarm, storage and other services. The system shall not be based on generic industry PC components and architectures.
 - 2. The recorder shall be part of a family of hybrid network video recorders consisting of 32, 24, 16, 8 and 4 channel variants.
 - 3. The 32 and 16 channel NVR platform shall have an option use docking station architecture, marrying a removable 2U-high NVR chassis (containing all system and video processing and storage components) with a fixed housing capable of mounting in a standard 19" equipment rack and accepting power, camera, network and other wiring connections.
 - 4. The 32-, 16-, 8- and 4-channel NVR platform shall have the option of using a rack shelf or desk top.

5. All of the NVR platforms shall also have the option of being mounted on a wall using optional wall mount kits. The 24-, 8- and 4-channel recorders shall further have an option for concealing the cabling using a tamper proof cover.
6. The NVR shall employ an embedded Linux operating system, housed in flash memory and capable of being upgraded remotely if needed, such that no system software shall be stored on hard-drive media, and the operating environment shall be more robust and immune to virus and illicit attack than other common operating systems. At the client desktop, however, all software applications shall support the latest Windows® operating environments.
7. The NVR shall provide for choice when selecting a software interface for either an integrated browser based client or a tasked based suite of installable clients.
8. Once a software interface has been selected, the NVR shall employ a common software interface regardless of the model selected. This will yield consistent user training materials, documentation and system interaction.
9. The NVR shall provide a 'hybrid' architecture, capable of supporting traditional analog cameras in the quantities shown below as well as a number of IP cameras (see below) to increase the aggregate camera support, provide high-resolution video capture in critical customer areas, and allow migration to this new camera technology according to customer need.

A. NVR Unit Configuration

The NVR unit shall be available in the following configuration common across all models:

1. The 32-, 24- and 16-channel units shall support 4 audio inputs, 2 which can support bi-directional, half-duplex input/outputs. The 8- and 4-channel units shall support 2 audio inputs, 1 which can support bi-directional, half-duplex input/outputs
2. The 32- and 16-channel units shall support 8 alarm inputs and 4 switch outputs. The 24-, 8- and 4- channel units shall support 2 alarm inputs and 1 switch outputs
3. 1 RS-232 ports,(all models), 1 RS-485,(32 and 16 channel units only) ports for integrating banking ATM/Teller transaction or retail POS transaction capture information and PTZ camera controllers, and 4 USB 2.0 (excluding 4 channel unit, which will support 2 USB 2.0 ports), (excluding 24 channel unit, which will support 3 USB 2.0 ports (1 internal)) data port for connecting keyboard, mouse, or external media for export purposes
4. 1 RJ-45 Gigabit Ethernet network connection for LAN-based system access and management
5. 1 RJ-45 Gigabit Ethernet network connection for connecting IP cameras and encoders on a network separate from the corporate LAN
6. The 24 channel unit includes 1 RJ-45 10/100 Base-T port for POS integrations and up to 24 PoE ports (RJ-45), 10/100 Base-T
7. The 32- and 16-channel units shall support up to 4 internal hard disk drives. The 24, 8-channel unit shall support up to 2 internal hard disk drives. All drives shall be high-capacity, SATA hard disk drives, supporting up to 10TB each. The 4 channel unit shall support up to 2 internal high-

capacity, SATA hard disk drives, supporting up to 5TB each. All drives shall be mounted for easy servicing.

8. 1 internal back-up battery for filtering out power fluctuations and provide controlled system shut down.
9. The 32- and 16-channel units shall support 2U-high docking-station chassis for simple mounting and servicing in a standard 19" equipment rack or a 2U-high desk top chassis if rack mounting is not required.
10. 16/8/4 BNC video inputs, dependent on model, (with software controlled loop-through capability) able to accept NTSC or PAL composite signals
11. The 24 channel unit will can be equipped with up to 24 HD analog inputs able to accept TVI, CVI or HDA signals.
12. The 32-, 16- and 8-channel units shall support 1 composite video output (NTSC or PAL) capable of displaying both analog and IP cameras in a programmable sequence.
13. The 32-, 24-, 16- and 8-channel units shall support 1 HDMI video output capable of displaying both analog and IP cameras in a high definition user interface for live display and archive searching.
14. 240 or 480 frame-per-second (FPS) aggregate video capture for the analog inputs (based on the model selected), supporting CIF and 4CIF video format [NOTE: Select only the unit necessary for the project]
15. The 24 channel unit can support 720 frame-per-second (FPS) aggregate video capture for the HD analog inputs supporting 1080P30.
16. Depending on the model selected, the total bandwidth available for IP cameras shall be shown in the table below:

32 Channel	24 Channel	16 Channel	8 Channel	4 Channel
96 Mbps	80 Mbps	48 Mbps	24 Mbps	12 Mbps

B. Configuration and Viewing Applications

The Visual Intelligence configuration and viewing applications shall be compatible with the latest version of Windows®. Each application shall be installed from a web download or USB using an automatic installation program. All applications shall have similar interfaces in order to reduce learning time and shall operate consistently across all members of the NVR product family.

The Command Enterprise configuration and viewing applications shall be compatible with the latest version of Windows® or MAC O/S. The integrated application shall be installed on the Command Enterprise server from a CD using an automatic installation program. Once installed on the Command Enterprise server, the application can be accessed by any operator on the network via a supported browser.

Concept of Operation

13. The NVR unit shall capture, digitize and compress video (using industry-standard H.264 video compression technology and multi-level encoding to further optimize transmitted and stored video) and, if desired, accompanying audio signals on all enabled inputs. Once compressed, the unit shall either distribute the compressed data to any number of authorized users requesting the data over either of the unit's network ports from one of the supported application interfaces (Command Enterprise or Visual Intelligence).
14. In parallel, the unit shall also store all compressed data to the available internal hard disk drive(s). These internal drives shall be expandable by the user, from a single drive configuration through to 4 high-capacity drives for extensive in-system storage. This in-system storage shall be capable of being set up in an offset mirrored configuration where 1 drive can be mirrored with up to 3 drives.
15. Certain models shall support Raid5 redundancy, supporting block level striping with distributed parity across 4 Hard Drives.
16. Internal system storage shall take advantage of Intelligent Video Archiving and Retention technology that uses the concept of retention rather than recording. A retention based system captures, by default, video from all connected cameras at the highest per-camera frame rates available on the unit (based on model selected), providing always-on high quality recording on all cameras in keeping with the FBI/Scientific Working Group on Image Technology [SWGIT] recommendations. The user shall then be able to set up rules to determine when the retained video is to be removed from the recorder and which video is to be retained.
17. After all of the attached storage has been filled, video of potential interest (e.g., motion video, alarm video, retail or financial transaction video) is reviewed according to the set rules and if tagged, is moved into the Longer-Term Storage area. All other video is removed and the disk space freed up by this 'thinning' process shall be available for new video storage. Beyond long-term storage, a further Extended-Term Storage area shall be available to further thin and retain critical video for an extended period of time.
18. At any time, selected video/audio data shall be available for export by users across the network to their PCs as well as through a USB-connected media storage device (e.g., USB memory stick or USB hard drive) at the NVR. This video shall be completely appropriate for use in evidentiary purposes and shall include a security (authentication) seal for continuity purposes and an auto-run Evidence Reviewer' utility for playback and assessment by third parties such as law enforcement officials.
19. The unit shall simultaneously handle recording, retrieving, and live distribution of video and audio. The unit shall operate in a continuous record mode, even if only event driven recordings, scheduled recordings or motion detection recordings are to be retained for longer periods of time. The unit must be capable of independent operation with network access and control, centralized management in conjunction with a number of other NVR units, or operation under the control of a centralized, enterprise-level suite of multiple-system management software.
20. The unit shall support operation in a local control mode where video can be viewed live and searched using only a mouse and a monitor connected to the HDMI connection. When operating in this mode, the unit does not have to be connected to a network except for the purpose of configuration of the unit. The local control interface shall support the export of

video clips to USB connected media. Local control support is not available on the 4 channel unit.

C. System Security

The unit shall be able to mount on a desktop, wall, or particularly for 32 and 16 channel units, inside a 19" equipment rack with a secure docking station, and have a removable but secured top cover such that the unit cannot be easily powered down or have the disk drive(s) accessed inappropriately.

Each NVR shall be deployed almost exclusively 'behind' an existing network security firewall, benefiting from the default virus protection software and encryption options of that equipment to prevent hacker attacks. In addition, the NVR shall be capable of existing securely on an unprotected network, thereby providing superior security performance relative to most other video systems available.

Each NVR shall use an embedded (in flash memory) Linux operating system, which is inherently more robust in architecture and less susceptible to virus and other "hacker" attacks than other operating systems. Each NVR shall minimize the number of access points for hackers to try and gain access to the unit or by which a virus may attack the unit. Communications with the NVR shall be very restricted, with most external ports being blocked and no way made available to open them. Communication between all entities in the system (client software, management server software, and NVRs) shall be encrypted using SSL encryption.

The NVR unit shall not share any known or unknown vulnerabilities associated with popular PC or computer operating systems. It shall achieve a C2 level of security. All TCP and UDP ports not required for use will be blocked thus ensuring that points of network attack will be minimized.

The NVR unit shall operate without the requirement for a keyboard, monitor or mouse - also known as 'headless' operation – instead being controlled across the network from authorized client PCs. As a result, no tampering shall be possible at the unit itself.

All analog video shall be captured and transmitted to the NVR over coaxial cables, directly connected to the rear of the units. No interception of these video streams shall be possible without physically tapping into the specific cable inside the customer premises.

All IP-camera-based video shall be captured and transmitted to the NVR using the IP protocol. The NVR shall have the capability of connecting with the cameras either through a routed network or directly via the IP camera card.

The NVR unit shall allow for the use of password authentication to prevent unauthorized access to the NVR. Two levels of authentication shall be supported (user and administrator) when the NVR is managed in a peer-to-peer fashion. When the NVR is being managed by server-based management software, the system shall support a large number of users and user groups, as well as a rich set of privileges. In this enterprise configuration, external user authentication using an existing enterprise application shall also be supported, providing the net effect for users of 'single sign-on' or single authentication through their traditional

system access utility.

The NVR shall ensure command and control data packets are encrypted for network transmission using SSL security technology NVR.

The system shall provide the ability to limit operator access to NVR resources. Administrators shall be able to manage user rights to a fine granularity of control, down to the level of access to the individual resource (for example, a single camera, audio channel, or data port).

The local or centralized system administrator shall be able to access all NVR units that are visible on the network, subject to each user's privilege level. Each individual NVR unit shall keep a log of any user access to the unit. The log shall be retrievable remotely by an administrator, but no user will be able to remove entries from the log. The log shall be maintained automatically by removing entries that are six months old. It shall be an option to copy and save the report to a text-formatted file for import into a third party application. It shall be an option to print the report. These capabilities shall be scalable such that they will work seamlessly under the control of a centralized, enterprise-level suite of multiple-system management software.

D. System Management

All NVR units shall be capable of being managed locally or centrally over a TCP/IP LAN or WAN network, using individual system or enterprise-level management utilities. All systems shall be capable of being managed by a set of consistent user interface applications that operate consistently across all members of the NVR product family. The enterprise-level management application shall be capable of managing system programming, monitoring the health of the system in real-time, of upgrading the software on an NVR unit, synchronizing the time on an NVR unit, remotely managing an NVR unit, and more.

Reports on systems use, problems, and alarms shall be capable of being printed. Reports shall also be capable of being copied or saved for importing into third party applications.

E. Automated Configuration

As NVR units are added to the network, the NVR management application shall automatically detect their presence on the network to support rapid configuration and administration.

F. Reliability

1. The NVR shall use an embedded (in flash memory) Linux operating system, which is inherently more robust in architecture and reliability than other operating systems.
2. No NVR operating software shall reside on the NVR hard-drives, eliminating hard-drive failure as a reliability issue and allowing the unit to operate without any hard-drives present (e.g., in a video streaming application, or when utilizing external storage).
3. The NVR unit shall contain hardware and software watchdog circuitry that maximize fault-free operation. The central management application shall report all problems detected by any NVR units on the network. The NVR configuration software shall continuously supervise the health of both the unit and the network, including dial-up extensions. The management utility shall periodically connect to all dial-up connected NVR units in order to ascertain the health of both the unit and the line/modem on which the unit is connected. An option to 'connect on demand' shall also be provided to support low-activity NVR deployments.

4. The NVR shall use SMART disk technology to provide real-time monitoring of all internal hard-disks, including diagnostics and health reporting, to provide further system reliability. The unit shall offer internal disk mirroring in a multi-drive configuration to further protect stored data.
5. The administrator shall control the level of problem reporting (thresholds) in order to ensure the reliability of the NVR and the equipment connected to the NVR unit, but also to manage the amount of communications consumed by this activity. The administrator shall be able to have notification of problems e-mailed to specific users.

G. Video Capture

1. The video compression protocol used by the NVR unit shall be H.264, which uses an inter-frame mechanism to assist in achieving the optimum compression.
2. The NVR shall have an aggregate capture rate of 240 or 480 fps (NTSC) or 200 or 400 fps (PAL) across its 4/8/16 analog inputs, depending on the model selected. The 24 channel unit shall have an aggregate capture rate of 720 fps at 1080P30. On all units, five (5) levels of compressed video quality shall be supported to balance desired video clarity against available hard drive storage.
3. Video capture rates shall be allocated in a flexible manner per camera, with different frame rate settings on each camera. Frame rates can be set anywhere from 1 fps up to 15 or 30 fps per camera input, respecting the limit of the model selected.
4. Per-camera video capture rates shall have the option of being increased (to the maximum available based on system capability) on alarm or event triggering (i.e., detection of motion, activation of a panic alarm button, etc.).
5. The NVR shall be capable of capturing and distributing video at high frame rates while storing at a lower frame rate or vice versa. Display resolutions shall be: NTSC - CIF (352 x 240 pixels), and 4CIF (704 x 480 pixels); PAL –CIF (352 x 288), and 4CIF (704 x 576).

H. Video Loss Detection

The NVR unit shall constantly supervise all enabled video inputs for a synchronization signal and, if enabled, notify the administrator of signal loss. Video sync loss detection shall be filtered to ensure that brief interruptions are masked and problem cameras do not generate excess alarms.

I. Field of View Monitoring

Using video analytic capabilities, the NVR unit shall also provide camera obstruction detection and scene change detection. Both applications will offer user-programmable learning parameters, and alert thresholds, and can be used together or independently.

J. Video Output

The NVR unit shall have looping video inputs plus a single video output (excludes video output on 24, 4 channel unit) which is capable of displaying video from selected camera inputs in a sequenced display application, with a programmable dwell sequence being available for each display. This sequence shall be interruptible in order to display specific video related to an event (i.e., alarm trigger) on the NVR unit, and shall return to the preset sequence once that event has completed.

K. Audio Capture

1. The 32-, 24- and 16-channel NVR shall provide the ability to record 4 channels of audio data synchronized with video data. Audio recording shall be 2-way, half-duplex communication on 2 of the channels. The 8 and 4 channel NVR shall provide the ability to record 2 channels of audio data synchronized with video data. Audio recording shall be 2-way, half-duplex communication on 1 of the channels. The audio compression protocol used shall be ADPCM compression. Four levels of Audio compression (quality) shall be supported.
2. Where audio recording is to accompany video capture, the video and audio shall be synchronized to within one second for both live viewing and playback.
3. Audio shall be recorded separate and distinct from the video such that it can be associated after with any video stream after it has been recorder.

L. Storage

1. The 32 and 16 channel NVR shall support 1 through to 4 internal hard disk drives. The 4 and 8 NVRs channel shall support 1 or 2 internal hard disk drives to provide high-capacity video storage, with the drives having a capacity of at least 3TB each or larger. The 4 channel unit shall support 1 or 2 internal hard disk drives to provide high capacity storage. With drives having a capacity of at least 1TB. No system (NVR) software or operating system elements shall reside on these hard drives, thereby avoiding any reduction in video storage capacity and increasing system robustness.
2. The NVR unit shall contain no removable media for off-line storage. All storage shall be on-line for as long a period as possible based on the configuration that has been selected. Configurable parameters for altering storage duration shall include:
 - Display size (CIF, 2CIF, 4CIF)
 - Frame rate
 - Video quality settings (most detailed, more detailed, medium, more compressed, most compressed)
3. Internal system storage shall take advantage of Intelligent Video Archiving and Retention technology that uses the concept of retention rather than recording. A retention based system captures, by default, video from all connected cameras at the highest per-camera frame rates available on the unit. This provides an always-on high quality recording on all cameras in keeping with the FBI/Scientific Working Group on Image Technology [SWGIT] recommendations. The user shall then be able to set up rules to determine when the retained video is to be removed from the recorder and which video is to be retained.
4. After all of the attached storage has been filled, video of potential interest (e.g., motion video, alarm video, retail or financial transaction video) is reviewed according to the set rules and if tagged, is moved into the, Longer-Term Storage area. All other video is removed and the disk space freed up by this 'thinning' process shall be available for new video storage. Beyond long-term storage, a further Extended-Term Storage area shall be available to further thin and retain critical video for an extended period of time.
5. All video shall be stored at the NVR unit and only be delivered over the network when either the recorded video is searched and retrieved or if live video is requested.

M. Recorded Information

The information recorded on the NVR unit shall consist of the following data:

1. Compressed video
2. Compressed audio
3. Time stamp consisting of date and time with millisecond resolution
4. Associated event information
5. Associated transaction information (for example, retail Point-of-Sale or ATM/Teller financial transactions)
6. Audit information

N. Recorded Format

Compressed video from all cameras shall be stored in such a way that it is independently retrievable. Compressed audio shall be stored in such a way that it is independently retrievable or can be associated with any video input. When a video recording with associated audio is retrieved, the audio shall be retrieved automatically (synchronized) along with the video. The operator shall be able to retrieve a video clip from the NVR unit at any file size up to a maximum of 2.0 GB.

O. Continuous Recording

The NVR unit shall be capable of recording continuously on each video and its audio input. The capacity for recording shall not exceed 40 GB when recording continuously for 7 days on 4 cameras at 15 fps, with a “More Compressed” setting and moderate to low motion. Capacity for recording on IP cameras shall be dependent on the configuration settings of the IP camera.

P. On-Event Recording

1. The NVR unit shall be capable of recording any video input (and associated audio if desired) in response to an external alarm. The recording period shall be of any duration from 30 seconds to seven days. There shall be no hard association of an external alarm to a camera or audio source. Any alarm can cause an action to record on any or all cameras and the audio input.
2. Optionally, any given camera shall be programmable to record at up to the maximum capture rate (fps) available from the system in response to an alarm.
3. Events that trigger long or extended-term retention shall include:
 - Any external closed current loop device connected to the NVR unit (door sensor, motion sensor, etc.)
 - Motion in the video image (in the image overall, or in individual and configurable ‘masked’ areas of the image, with configurable sensitivity settings)
4. Extended retention on video motion detection shall be tunable using full screen sensitivity setting to simplify configuration or using a user definable grid for area of interest. In order to reduce the frequency of motion alarms, the detection of next occurrence of motion can be delayed until there is a period of inactivity in the image. Detection of video motion shall be capable of being enabled during specific periods of the day according to a pre-determined schedule.

Q. Scheduled Recording

The NVR unit shall be capable of executing any number of internal recording schedules defined by the administrator. Schedules shall be remotely configurable and control the following actions:

1. Extended retention (any combination of cameras for any duration from 30 seconds to 7 days)
 2. Monitoring of physical alarms (during specified periods)
 3. Monitoring of motion alarms (during specified periods)
 4. Increase of the bandwidth throttle
 5. Assertion of a switch (for a specified period)
 6. Moving of a PTZ unit to a predefined position
 7. Displaying of a specific camera on the spot monitor
- R. Time Synchronization
- The NVR unit shall allow for clock synchronization to occur manually or from a central location through a network time protocol (NTP) server or enterprise management server. The NVR unit shall also be capable of automatically adjusting the clock to Daylight Saving Time, and adjusting for deployment in varying time zones.
- S. Live Video/Audio Viewing
- The NVR viewing application shall be capable of displaying up to 36 video windows simultaneously in a 6 x 6 grid with video from cameras on the same NVR as well as video from different NVRs. Live video windows shall be able to co-exist on one monitor or across several, with playback windows on the same screen from within the same application. Each video/audio window shall have independent control and all windows shall be capable of being linked together and controlled simultaneously. Each video/audio window shall be capable of performing an instant replay of selected duration by simply using a slider control to move back in time. If audio is associated with the selected window there shall be a set of controls to adjust the volume or mute the audio.
- T. Video Zoom/Full Screen Display
- The currently selected video window shall support digital zooming of 50 percent to 200 percent using pre-defined buttons. As well, wire frame selection of area to zoom shall also be supported with the ability to pan to areas of interest that are outside of the displayed window frame. The displayed video shall have an option to adjust to the size of the window frame. Multiple windows shall be capable of having the zoom and fit-to-screen operations applied simultaneously. Any single video window shall be capable of being displayed in full screen mode with no window frame (audio will continue to be heard in this mode).
- U. PTZ control
1. The NVR unit shall allow for connection to PTZ cameras through the RS-232 or RS-485 ports on the unit, and multiple PTZ cameras may be 'daisy-chained' on a single port as defined by the PTZ protocol the user deploys (see #2 below). Control of these cameras shall be possible on the operator side through a physical connection to a PTZ controller (keypad/joystick) or through on-screen software controls. On-screen software controls shall allow for selection of PTZ camera to control, direction of camera movement, zoom, focus and configuration of camera preset locations.
 2. At a minimum, the following PTZ camera protocols shall be supported on the NVR:
 - Kalatel® KTD-312
 - Panasonic® WV-CS850

- Pelco® D
- Pelco® P
- Phillips® TC700/TC8560
- RVision®
- Sony® UniDome UNI-TR1
- Ultrak® KD-6

V. Video Image Settings

The video window shall support image controls for brightness, contrast, saturation, and hue levels to customize the appearance of video in the active display window. Recorded video is in no way altered by these controls, however, printed or saved still images can be image enhanced.

W. Dataports

The NVR unit shall be able to capture and store banking ATM/Teller or retail Point-of-Sale (POS) transaction information using the RS-232 data port or 10/100 base T RJ-45 connection available on the unit. The text information captured from a transaction system shall not overlay or obstruct the video in any way, but shall be synchronized with that video, and shall serve as a trigger to capture recorded video of preset duration (including pre-transaction video).

X. Switch Control

The NVR viewer shall be able to manually control devices connected to the switch output of the NVR unit by activating one either normally open (NO) or normally closed (NC) contact. The switch shall automatically reset after a configurable period of time. The switch shall also be set in response to an external event occurring or as a scheduled operation.

Y. Alarm Notification

The NVR unit shall distribute notification of alarms to clients who have requested notification. All video associated with the alarm shall be automatically displayed on receipt of an alarm. Audible and visual alarm cues shall also be optionally configurable. An operator shall be able to have notification of alarms e-mailed to specific users.

Z. Time Zones

The NVR unit shall be capable of operating in a different time zone than a viewing application. The operator shall be able to work in either the time zone of their PC or the time zone of the NVR when searching for video. Operator software shall display either the local (user) time zone, or the time zone of the NVR when displaying video timestamps.

AA. Search of Alarms

1. Video recorded on alarms shall be searchable by selecting the alarm of interest and entering a specific point in time and period of interest. Each type of alarm shall have a unique icon to represent it in the list. An operator shall be able to narrow down the search without having to re-enter all the parameters. All alarm-associated recordings (i.e. all cameras) shall be retrieved and displayed by selecting a specific entry from the alarm search results. The duration of retrieved video surrounding the alarm point shall be configurable by each user.
2. Video motion alarms shall be handled in the same way as other physical alarms. A mask shall be able to be applied to a search for video motion such that the results list displays only when motion was detected in the area(s) of interest.
3. Transaction events captured from an ATM or bank Teller machine interface shall be handled in the same way as other physical alarms, in that they shall be searchable by date and time as

well as other custom user data. The search fields for ATM/Teller transaction alarms shall include:

- Transaction type
 - Transaction number
 - Transaction amount
 - Card number
 - Time/date stamp
 - Other custom field
5. Transaction events captured from a Point-of-Sale (POS) retail interface shall be handled in the same way as other physical alarms, in that they shall be searchable by date and time as well as other custom user data. The search fields for POS transaction alarms shall include:
- Transaction type
 - Transaction number
 - Transaction amount
 - Card number
 - Time/date stamp
 - Other custom field
6. A range will be used when searching on either transaction amounts (e.g., from \$1000.00 to \$5000.00, or from \$0.00 to \$100.00, with a maximum of \$1,000,000.00).

BB. Search and Retrieval of Recordings

1. Searching and retrieving video and audio from the NVR unit shall be done as a single operation (i.e. if the audio is associated with the video, it will be retrieved as well).
2. The search function shall allow multiple cameras, multiple NVRs, or multiple NVR locations to be specified and searched simultaneously.
3. Recorded video shall be searchable by:
 - Selecting the camera of interest and entering a range of times. The user shall be able to further refine this range by a simple “click-and-drag” operation, and not have to re-enter any search parameters. The user shall be presented with a histogram indicating the amount of motion during the time range, as well as a set of thumbnails to aid in pinpointing a time of interest.
 - Selecting an alarm and using the specific point in time of the alarm to locate the associated video
 - Using the ‘activity scan’ feature to search based on motion detection
 - Specifying ATM or POS transaction data as mentioned above
7. The search function shall allow any duration of video to be retrieved (to a maximum file size of 2.0 GB).

CC. Playback Viewing

The retrieved video shall be displayed automatically in a window. The playback windows shall be capable of being displayed alongside the live video windows. If audio is associated with the video that is retrieved, it shall be automatically played when the video is played. A date/time stamp shall appear with the video being displayed and shall be updated for each frame that is displayed.

DD. Playback Controls

1. When a playback window is selected, the following controls shall be made available to control the playback of the video:
 - Play – forward and reverse
 - Pause
 - Single frame – forward and reverse.
 - Move to beginning to ending of video segment
8. In addition, the play speed shall be capable of being changed to 1x, 2x, and 4x normal speed. The recorded video shall also be capable of being quickly navigated using a shuttle search (slide bar). Video frames shall be displayed while the slide bar is being moved to assist in finding the frame of interest.

EE. Time Ruler

For navigation through a video clip, the operator shall be able to use a slide bar. The video image shall update while the slide bar is being moved. To change the time resolution for more accurate navigation, the time ruler shall be capable of being zoomed in or out.

FF. Video Images - Copy, Save and Print

An image from a live or playback video window shall be capable of being manipulated as follows:

1. The image shall be capable of being copied to the PC 'clipboard' and then pasted into any third party application that will accept data from that clipboard. These applications include image enhancement, email, or word processing. Image copying options shall include specifying standard JPEG or .BMP file formats for the image. The copied information shall include both video and associated detail data (location, camera, time, date, and event information).
2. The resulting images shall then be able to be saved to the local PC or other network storage location, retaining their JPEG or .BMP file formats and their associated detail data.
3. The images shall also be capable of being printed to any network-connected printer. The printed image shall have the associated detail data (location, camera, time, and date) printed on the same page.

GG. Video Clips – Security Sealed

A video clip from a live or playback video window shall be capable of being controlled as follows:

1. The video clip shall be capable of being saved to the local PC or other network storage location in an industry-standard .AVI read-only file format. The captured information shall include the video clip itself, any audio data if recorded, and associated location, camera, time, date and event details, as well as any captured POS or ATM transaction data.
2. All video clips shall have a tamper-proof security seal applied automatically as part of this process, ensuring the authenticity of that video and its admissibility as evidence in a legal

investigation or prosecution process. This security seal process shall be based on the SHA (Secure Hash Algorithm) of Digital Signature Standard [U.S. FIPS PUB 180-1, 1995].

3. Video clips shall be able to be exported from the NVR to a USB-connected CD Burner or memory stick. Control of this operation shall be made available to authorized clients locally or remotely over the network. This export process shall include the copying of a free, auto-run Evidence Reviewer utility with which third parties may play back the video clip. Users of the Evidence Reviewer utility shall have the ability to run the utility directly from the media, without requiring them to install it on their workstations.
4. The industry-standard .AVI video files shall be capable of being displayed by any commercial application that will render such media files. To display all associated detail data, and to verify authenticity of the video, the Evidence Reviewer utility shall be necessary.

PART 3 EXECUTION

3.1 EXAMINATION

- A. Do not begin installation until substrates have been properly prepared.
- B. Examine site conditions prior to installation. Notify Architect and Owner in writing if unsuitable conditions are encountered. Do not start installation until site conditions are acceptable.
- C. If preparation is the responsibility of another installer, notify Architect in writing of deviations from manufacturer's recommended installation tolerances and conditions.

3.2 INSTALLATION

- A. All components of the recorder shall be thoroughly tested before shipping to the project location.
- B. Recorder shall be installed, programmed and tested in accordance with manufacturer's installation instructions.
 1. Coordinate interfaces with Owner's representative where appropriate.
 2. Provide backboxes, racks, connectors, supports, conduit, cable, and wire for a complete and reliable installation. Obtain Owner's approval for exact location of all boxes, conduit, and wiring runs prior to installation.
 3. Install conduit, cable, and wire parallel and square with building lines, including raised floors areas. Do not exceed forty percent (40 percent) fill in conduits. Gather wires and tie to create an orderly installation.
 4. Coordinate with other trades to provide proper sequencing of installation.

3.3 FIELD COMMISSIONING

- B. Test recorder as recommended by manufacturer, including the following:

1. Conduct complete inspection and testing of equipment, including verification of operation with connected equipment.
2. Test devices and demonstrate operational features for Owner's representative and authorities having jurisdiction, as applicable.
3. Correct deficiencies until satisfactory results are obtained.
4. Submit written copies of test results.

3.4 TRAINING AND CERTIFICATION

- A. The recorder manufacturer shall offer free online training for authorized dealer technicians through user controlled portal access.
- F. Training material shall cover all aspects of installation, configuration and maintenance.
- G. The dealer shall receive a certificate upon the successful completion of the certification exam. Certifications shall be valid for a period of 2 years.
- H. The recorder manufacturer shall offer free online training tutorials for system administrators accessible 24/7 via open (non-restricted) website for an unlimited number of system users. The training tutorial shall cover the system, User management, Health alert management and Mass Management (upgrades) of all registered devices on the recorder.
- I. The recorder manufacturer shall offer free online training for Guards and Investigators accessible 24/7 via open (non-restricted) website for an unlimited number of system users. The training tutorial shall cover system access, live and archive media requests, alarm inbox management, as well as extracting media from the system

END OF SECTION

Axis IP Cameras

GENERAL

The CCTV cameras installed at City of Brampton sites are to be manufactured by Axis Communications.. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.4 of this document.

1.01 SYSTEM DESCRIPTION

General Requirements

1. The specified unit shall be of manufacturer's official product line, designed for commercial and/or industrial 24/7/365 use.
2. The specified unit shall be based upon standard components and proven technology using open and published protocols.

A. Sustainability

1. The specified unit shall be manufactured in accordance with ISO 14001.
2. The specified unit shall be compliant with the EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE).
3. The specified unit shall be compliant with the EU regulation 1907/2006 (REACH).

1.02 CERTIFICATIONS AND STANDARDS

B. General abbreviations and acronyms

1. AGC: Automatic gain control
2. API: Application Programming Interface
3. Aspect ratio: A ratio of width to height in images
4. Bit Rate: The number of bits/time unit sent over a network
5. Bonjour: Enables automatic discovery of computers, devices, and services on IP networks.
6. DHCP: Dynamic Host Configuration Protocol
7. DNS: Domain Name System
8. EIS: Electronic Image Stabilization
9. FPS: Frames per Second
10. FTP: File Transfer Protocol
11. H.264 (Video Compression Format)
12. IEEE 802.1x: Authentication framework for network devices
13. IP: Internet Protocol
14. IR light: Infrared light
15. JPEG: Joint Photographic Experts Group (image format)
16. LAN: Local Area Network
17. LED: Light Emitting Diode
18. Lux: A standard unit of illumination measurement
19. MBR: Maximum Bit Rate
20. MPEG: Moving Picture Experts Group
21. Multicast: Communication between a single sender and multiple receivers on a network
22. NTP: Network Time Protocol
23. NTSC: National Television System Committee – a color encoding system based on 60Hz

24. ONVIF: Global standard for the interface of IP-based physical security products
25. PAL: Phase Alternating Line – a color encoding system based on 50Hz
26. PoE: Power over Ethernet (IEEE 802.3af/at) standard for providing power over network cable
27. Progressive scan: An image scanning technology which scans the entire picture
28. PTZ: Pan/Tilt/Zoom
29. QoS: Quality of Service
30. SIP: Session Initiation Protocol
31. SMTP: Simple Mail Transfer Protocol
32. SMPTE: Society of Motion Picture and Television Engineers
33. SNMP: Simple Network Management Protocol
34. SSL: Secure Sockets Layer
35. TCP: Transmission Control Protocol
36. TLS: Transport Layer Security
37. Unicast: Communication between a single sender and single receiver on a network
38. UPnP: Universal Plug and Play
39. UPS: Uninterruptible Power Supply
40. VBR: Variable Bit Rate
41. VMS: Video Management System
42. WDR: Wide dynamic range

A. The specified unit shall carry the following EMC approvals:

1. EN55022 Class A, EN55024, EN61000-6-1, EN61000-6-2
2. FCC Part 15 - Subpart B Class A
3. VCCI: 2014, Class A, ITE
4. C-tick AS/NZS CISPR22 Class A
5. ICES-003 Class A
6. KCC KN22 Class A, KN24

B. The specified unit shall meet the following product safety standards:

1. IEC/EN/UL 60950 -1
2. IEC/EN/UL 60950-22

C. The specified unit shall meet relevant parts of the following video standards:

1. SMPTE 296M (HDTV 720p)

D. The specified unit shall meet the following standards

1. MPEG-4:
 - a. ISO/IEC 14496-10 Advanced Video Coding (H.264)
2. Networking:
 - a. IEEE 802.3af/802.3at (Power over Ethernet)
 - b. IEEE 802.1X (Authentication)
 - c. IPv4 (RFC 791)
 - d. IPv6 (RFC 2460)
 - e. QoS – DiffServ (RFC 2475)
3. Network video
 - a. Relevant ONVIF profile as defined by the ONVIF Organization.
4. Mechanical Environment:

- a. IEC/EN 60529 IP66 & IP67
- b. NEMA 250 Type 4X
- c. IEC/EN 62262 IK08
- d. IEC 60068-2-6
- e. IEC 60068-2-27

1.03 QUALITY ASSURANCE

1. The Contractor or security sub-contractor shall be a licensed security Contractor with a minimum of five (5) years' experience installing and servicing systems of similar scope and complexity and evidence that is completed at least three (3) projects of similar design and is currently engaged in the installation and maintenance of systems herein described.
2. All installation, configuration, setup, program and related work shall be performed by electronic technicians thoroughly trained by the manufacturer in the installation and service of the equipment provided.
3. The contractor or designated sub-contractor shall submit credentials of completed manufacturer certification, verified by a third party organization, as proof of the knowledge.
4. The Contractor shall provide four (4) current references from clients with systems of similar scope and complexity that became operational in the past three (3) years.
5. The specified unit shall be manufactured in accordance with ISO9001.

1.04 WARRANTY

- a. All security system components and labor furnished by the contractor including wiring, software, hardware and custom parts shall be fully warranted for parts, materials, labor and travel expenses for a minimum of three (3) years from date of the final acceptance of the Video Surveillance System.
- b. The manufacturer shall provide warranty and optional extended warranty for the camera for a total period of maximum five years. If enacted as part of the contract, the contractor will repair or replace parts and/or labor per the warranty for the length of this warranty at no cost to the client.

Part 2: PRODUCTS

2.01 General

- a. Cameras shall be IP-based and comply with established network and video standards.
- b. Cameras shall be powered by the switch utilizing the network cable. Power injectors (midspans) shall be provided by the contractor when required for proper operation.
- c. Cameras shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
- d. Network door stations shall comply with relevant ONVIF profile as defined by the ONVIF Organization.

2.02 Video Surveillance schedule

- a. Camera types listed below describing various resolutions, form-factor and features shall be supplied by a single camera manufacturer.
- b. The camera manufacturer and model numbers will be as follows:
 1. Indoor low end fixed shall be Axis M3026-VE
 2. Indoor Fixed Dome shall be Axis P3225-LV MKII
 3. Outdoor Fixed Dome shall be Axis P3225-LVE MKII
 4. Indoor Fixed Minidome shall be Axis M3044-V
 5. Indoor/Outdoor PTZ shall be Axis M5525-E
 6. 720P PTZ shall be Axis P5634-E MKII
 7. Outdoor 1080P PTZ shall be Axis Q6055-E
 8. 360 degree Multi-sensor (4) with optional PTZ shall be Axis Q6000-E

1.03 video surveillance cameras

A. Fixed dome 3Mpxl network camera

1. The fixed dome network camera shall meet or exceed the following design specifications:
 - a. The camera shall operate on an open source; Linux-based platform and including a built-in web server.
 - b. The camera shall be equipped with an IR-sensitive progressive scan megapixel sensor.
 - c. The camera shall provide a removable IR-cut filter, providing day/night functionality.
 - d. The camera shall provide local video storage utilizing a microSD/microSDHC/microSDXC memory card expansion, supporting memory up to 64 GB.
 - e. The camera shall be manufactured with an IP66- and NEMA 4X-rated, IK10 impact-resistant aluminum casing.
 - f. The camera shall provide a manual 3-axis (pan/tilt/rotation) positioning to allow adjustment for optimum camera rotation and placement.
2. The fixed dome network camera shall meet or exceed the following performance specifications:
 - a. Illumination
 1. The camera shall meet or exceed the following illumination specifications:
 - a. 0.3 lux in color
 - b. 0.06 lux in B/W
 - b. Resolution
 1. The camera shall be designed to provide individually configured video streams in 3 MP (2048x1536) at 16/20 frames per second in power line frequency 50/60 Hz, using H.264 or Motion JPEG.
 2. The camera shall support video resolutions including:
 - a. 2048x1536
 - b. 1920x1080 (HDTV 1080p)
 - c. 1600x1200
 - d. 1280x1024
 - e. 1280x960
 - f. 1280x720 (HDTV 720p)

3. The camera shall provide both landscape format (4:3 and 16:9 aspect ratio) as well as corridor format (3:4 and 9:16 aspect ratio).

c. Encoding

1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 16/20 frames per second at capture mode 3 MP (2048x1536), up to 25/30 frames per second at capture mode 2 MP (1600x1200 and up to 25/30 frames per second at capture mode HDTV 1080p (1920x1080).
 - b. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in a selectable range from 1 up to 16/20 frames per second at capture mode 3 MP (2048x1536), up to 25/30 frames per second at capture mode 2 MP (1600x1200 and up to 25/30 frames per second at capture mode HDTV 1080p (1920x1080).
 - c. Baseline Profile H.264 encoding with motion estimation in a selectable range from 1 up to 16/20 frames per second at capture mode 3 MP (2048x1536), up to 25/30 frames per second at capture mode 2 MP (1600x1200 and up to 25/30 frames per second at capture mode HDTV 1080p (1920x1080)
2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate speaks the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
4. The camera shall provide configurable compression levels.
5. Support motion estimation in H.264/MPEG-4 Part 10/AVC.

d. Transmission

1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.

e. Image

1. The camera shall incorporate Automatic and Manual White Balance.
2. The camera shall incorporate an electronic shutter operating in the range of 1/30500 s to 2 s.
3. The camera shall incorporate capture mode with the following settings:
 - a. 2 MP (1600x1200) and HDTV 1080p (1920x1080) - 25/30 fps
 - b. 3 MP - 16/20 fps
4. The camera shall incorporate Wide Dynamic Range – Dynamic contrast.
5. The camera shall provide backlight compensation functionality.
6. The camera shall support manually defined values for:

- a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
- 7. The camera shall incorporate a function for optimization of low light behavior.
- 8. The camera shall allow for rotation of the image in steps of 90°.
- f. User Interface
 - 1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as Verisign, Inc.
 - 2. Language Specification
 - a. The camera shall provide a function for altering the language of the user interface and shall include support for at least 10 different languages.
 - 3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.
 - b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- g. PTZ functionality
 - 1. The camera shall:
 - a. Provide Digital PTZ functionality.
 - b. Provide:
 - 1. Pan: $\pm 175^\circ$
 - 2. Tilt 70°
 - 3. Rotation $\pm 180^\circ$
- h. Event functionality
 - 1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection
 - b. Live Stream Accessed
 - c. Camera tampering
 - d. Manual Trigger/Virtual Inputs
 - e. PTZ functionality
 - f. External input
 - g. Embedded third party applications
 - h. Edge storage disruption detection

2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP, SNMP trap or email
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email
 - d. Recording to local storage and/or network attached storage
 - e. Activating external output
 - f. PTZ control functionality
3. The camera shall provide memory for pre & post alarm recordings.
- i. Edge storage
 1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras SD-card slot
 - b. Network attached storage, located on the local network
 2. The camera shall be able to detect and notify Edge storage disruptions.
- j. Protocol
 1. The camera shall incorporate support for at least IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, SSH, NTP, CIFS/SMB, Bonjour.
 2. The SMTP implementation shall include support for SMTP authentication.
- k. Text overlay
 1. The camera shall:
 - a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
 - b. Provide the ability to apply privacy masks to the image.
 - c. Allow for the overlay of a graphical image, such as a logotype, into the image.
- l. Security
 1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
 2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
 3. The camera shall support IEEE 802.1X authentication.
 4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
 5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.
- m. API support
 1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
 2. The camera shall support relevant ONVIF profiles as defined by the ONVIF Organization.

n. Embedded applications

1. The camera shall provide a platform allowing the upload of third party applications into the camera.

o. Installation and maintenance

1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.
6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.

p. Access log

1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.
2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.

q. Camera diagnostics

1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
3. The camera shall send a notification when the unit has re-booted and all services are initialized.

r. Hardware interfaces

1. Network interface

- a. The camera shall be equipped with one 100BASE-TX Fast Ethernet-port, using a standard male RJ45 connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).

2. Inputs/Outputs

- a. The camera shall be equipped with one digital (alarm) input and one digital output, accessible via a removable terminal block. This input shall be configurable to respond to normally open (NO) or normally closed (NC) dry contacts.

s. Enclosure

1. The camera shall:
 - a. Be manufactured with an IP66- and NEMA 4X-rated, IK10 impact-resistant aluminum casing.
 - b. Be fitted with a clear transparent cover
 - c. Be equipped with a preinstalled 2 m (6.6 ft) network cable.
 - t. Power
 1. Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 2
 - u. Environmental
 1. Operate in a temperature range of -30 °C to +50 °C (-22 °F to 122 °F).
 2. Operate in a humidity range of 10–100% RH (condensing).
- B. Fixed indoor dome 1080p network camera
1. The fixed dome network camera shall meet or exceed the following design specifications:
 - a. The camera shall operate on an open source; Linux-based platform and including a built-in web server.
 - b. The camera shall be equipped with an IR-sensitive progressive scan megapixel sensor.
 - c. The camera shall provide a removable IR-cut filter, providing day/night functionality.
 - d. The camera shall be equipped with a varifocal lens with P-iris.
 - e. The camera shall provide local video storage utilizing a microSD/microSDHC/microSDXC memory card expansion.
 - f. The camera shall be manufactured with an IP52-rated, IK08 impact-resistant, polycarbonate casing.
 - g. The camera shall provide a manual 3-axis (pan/tilt/rotation) positioning to allow adjustment for optimum camera rotation and placement.
 - h. The camera shall provide options for clear and smoked lower dome.
 2. The fixed dome network camera shall meet or exceed the following performance specifications:
 - a. Illumination
 1. The camera shall meet or exceed the following illumination specifications:
 - a. HDTV 1080p 25/30 fps with WDR - forensic capture
 1. 0.16 lux at 50 IRE, F1.4 (color)
 2. 0.03 lux at 50 IRE, F1.4, 0 lux with IR illumination on (B/W)
 - b. HDTV 1080p 50/60 fps without WDR - forensic capture
 1. 0.32 lux at 50 IRE, F1.4 (color)
 2. 0.06 lux at 50 IRE, F1.4, 0 lux with IR illumination on (B/W)
 2. Camera shall have Lightfinder Technology
 - b. Resolution
 1. The camera shall be designed to provide at least two video streams in HDTV 1080p (1920x1080) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG (WDR inactive).

2. The camera shall be designed to provide at least two video streams in HDTV 1080p (1920x1080) at up to 30 frames per second (60Hz mode) or 25 frames per second (50Hz mode) using H.264 or Motion JPEG (WDR active).
 3. The camera shall be designed to provide 2 individually cropped out view areas.
 4. The camera shall support video resolutions including:
 - a. 1920x1080 (HDTV 1080p)
 - b. 1280x960
 - c. 1280x720 (HDTV 720p)
 - d. 1024x768
 - e. 1024x640
 5. The camera shall provide both landscape format (4:3 and 16:9 aspect ratio) as well as corridor format (3:4 and 9:16 aspect ratio).
- c. Encoding
1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 25/30 frames per second.
 - b. Motion JPEG encoding in a selectable range from 1 up to 50/60 frames per second.
 - c. Baseline Profile H.264 encoding with motion estimation in up to 25/30 frames per second.
 - d. Baseline Profile H.264 encoding with motion estimation in up to 50/60 frames per second.
 - e. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 25/30 frames per second.
 - f. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 50/60 frames per second.
 - g. Support High Profile H.264 encoding with motion estimation up to 25/30 frames per second.
 - h. Support High Profile H.264 encoding with motion estimation up to 50/60 frames per second.
 - i. Support H.264 with automatic scene adaptive bitrate control.
 2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
 3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate spikes the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
 4. The camera shall provide configurable compression levels.
 5. Support standard baseline profile H.264 with motion estimation.
 6. Support motion estimation in H.264/MPEG-4 Part 10/AVC.
 7. The camera shall have Zipstream technology, an H.264 implementation that supports scene adaptive bitrate control with the following capabilities to lower bandwidth and storage.
 - a. Automatic dynamic Region of Interest to reduce bitrate in unprioritized regions in order to lowering bandwidth and storage requirements.

- b. Automatic dynamic Group of Pictures to lower bandwidth and storage requirements
 - c. Automatic dynamic Frames per Second to lower bandwidth and storage requirements
- d. Transmission
 - 1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
 - 2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.
- e. Image
 - 1. The camera shall incorporate Automatic and Manual White Balance.
 - 2. The camera shall incorporate an electronic shutter operating in the range of 1/66500 s to 1 s.
 - 3. The camera shall incorporate capture mode with the following settings:
 - a. 25/30 fps (WDR-Forensic Capture) (50/60 Hz)
 - b. 50/60 fps (no WDR-Forensic Capture) (50/60 Hz)
 - 4. The camera shall incorporate Wide Dynamic Range - Forensic Capture functionality providing up to 120dB dynamic range.
 - 5. The camera shall support manually defined values for:
 - a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
 - 6. The camera shall incorporate a function for optimization of low light behavior.
 - 7. The camera shall allow for rotation of the image in steps of 90°.
- f. IR Illumination
 - 1. The camera shall be equipped with built-in IR LEDs with adjustable illumination intensity.
 - a. The IR LEDs shall have a range of up to 30 m (100 ft).
 - b. The IR LEDs shall emit light with a wavelength of 850 nm.
- g. User Interface
 - 1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as Verisign, Inc.
 - 2. Language Specification

- a. The camera shall provide a function for altering the language of the user interface, and shall include support for at least 10 different languages.
- 3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.
 - b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- h. PTZ functionality
 - 1. The camera shall:
 - a. Provide Digital PTZ functionality.
- i. Event functionality
 - 1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection
 - b. Live Stream Accessed
 - c. Day/Night Mode
 - d. Camera tampering
 - e. Manual Trigger/Virtual Inputs
 - f. PTZ functionality
 - g. Embedded third party applications
 - h. Edge storage disruption detection
 - 2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP, SNMP trap or email
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email
 - d. Send SNMP trap message
 - e. Activate/Deactivate IR Illumination
 - f. Recording to local storage and/or network attached storage
 - g. PTZ control functionality
 - h. WDR mode
 - 3. The camera shall provide memory for pre & post alarm recordings.
- j. Edge storage
 - 1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras microSD-card slot
 - b. Network attached storage, located on the local network
 - 2. The camera shall be able to detect and notify Edge storage disruptions.
- k. Protocol

1. The camera shall incorporate support for at least IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, SSH, NTP, CIFS/SMB, Bonjour.
 2. The SMTP implementation shall include support for SMTP authentication.
- l. Text overlay
1. The camera shall:
 - a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
 - b. Provide the ability to apply privacy masks to the image.
 - c. Allow for the overlay of a graphical image, such as a logotype, into the image.
- m. Security
1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
 2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
 3. The camera shall support IEEE 802.1X authentication.
 4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
 5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.
- n. API support
1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
 2. The camera shall support relevant ONVIF profiles as defined by the ONVIF Organization.
- o. Embedded applications
1. The camera shall provide a platform allowing the upload of third party applications into the camera.
- p. Installation and maintenance
1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
 2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
 3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
 4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
 5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.

6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.
 7. The camera shall provide Remote zoom and Remote focus functionality.
- q. Access log
1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.
 2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.
- r. Camera diagnostics
1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
 2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
 3. The camera shall send a notification when the unit has re-booted and all services are initialized.
- s. Hardware interfaces
1. Network interface
 - a. The camera shall be equipped with one 10BASE-T/100BASE-TX PoE Fast Ethernet-port, using a standard connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).
- t. Enclosure
2. The camera shall:
 - a. Be manufactured with an IP52-rated, IK08 impact-resistant, polycarbonate casing.
 - b. Be fitted with a dehumidifying membrane.
 - c. Providing encapsulated electronics and captive screws.
- u. Power
1. Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3
 - a. Max: 10.2 W
 - b. Typical 6.1 W
- v. Environmental
1. Operate in a temperature range of 0 °C to +50 °C (+32 °F to 122 °F).
 2. Operate in a humidity range of 10–85% RH (non-condensing).
- C. Fixed outdoor dome 1080p network camera
1. The fixed dome network camera shall meet or exceed the following design specifications:
 - a. The camera shall operate on an open source; Linux-based platform, and including a built-in web server.
 - b. The camera shall be equipped with an IR-sensitive progressive scan megapixel sensor.
 - c. The camera shall provide a removable IR-cut filter, providing day/night functionality.

- d. The camera shall be equipped with a varifocal lens with P-iris.
 - e. The camera shall provide local video storage utilizing a microSD/microSDHC/microSDXC memory card expansion.
 - f. The camera shall be manufactured with an IP66- and NEMA 4X-rated, IK10 impact-resistant casing.
 - g. The camera shall provide a manual 3-axis (pan/tilt/rotation) positioning to allow adjustment for optimum camera rotation and placement.
 - h. The camera shall provide options for clear and smoked lower dome.
2. The fixed dome network camera shall meet or exceed the following performance specifications:
- a. Illumination
 - 1. The camera shall meet or exceed the following illumination specifications:
 - a. HDTV 1080p 25/30 fps with WDR - forensic capture
 - 1. 0.16 lux at 50 IRE, F1.4 (color)
 - 2. 0.03 lux at 50 IRE, F1.4, 0 lux with IR illumination on (B/W)
 - b. HDTV 1080p 50/60 fps without WDR - forensic capture
 - 1. 0.32 lux at 50 IRE, F1.4 (color)
 - 2. 0.06 lux at 50 IRE, F1.4, 0 lux with IR illumination on (B/W)
 - 2. Camera shall have Lightfinder Technology
 - b. Resolution
 - 1. The camera shall be designed to provide at least two video streams in HDTV 720p (1280x720) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG (WDR inactive).
 - 2. The camera shall be designed to provide at least two video streams in HDTV 720p (1280x720) at up to 30 frames per second (60Hz mode) or 25 frames per second (50Hz mode) using H.264 or Motion JPEG (WDR active).
 - 3. The camera shall be designed to provide 2 individually cropped out view areas.
 - 4. The camera shall support video resolutions including:
 - a. 1920x1080 (HDTV 1080p)
 - b. 1280x960
 - c. 1280x720 (HDTV 720p)
 - d. 1024x768
 - e. 1024x640
 - 5. The camera shall provide both landscape format (4:3 and 16:9 aspect ratio) as well as corridor format (3:4 and 9:16 aspect ratio).
 - c. Encoding
 - 1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 25/30 frames per second.
 - b. Motion JPEG encoding in a selectable range from 1 up to 50/60 frames per second.
 - c. Baseline Profile H.264 encoding with motion estimation in up to 25/30 frames per second.

- d. Baseline Profile H.264 encoding with motion estimation in up to 50/60 frames per second.
 - e. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 25/30 frames per second.
 - f. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 50/60 frames per second.
 - g. Support High Profile H.264 encoding with motion estimation up to 25/30 frames per second.
 - h. Support High Profile H.264 encoding with motion estimation up to 50/60 frames per second.
 - i. Support H.264 with automatic scene adaptive bitrate control.
- 2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
- 3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate spikes the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
- 4. The camera shall provide configurable compression levels.
- 5. Support standard baseline profile H.264 with motion estimation.
- 6. Support motion estimation in H.264/MPEG-4 Part 10/AVC.
- 7. The camera shall have Zipstream technology, an H.264 implementation that supports scene adaptive bitrate control with the following capabilities to lower bandwidth and storage.
 - a. Automatic dynamic Region of Interest to reduce bitrate in unprioritized regions in order to lowering bandwidth and storage requirements.
 - b. Automatic dynamic Group of Pictures to lower bandwidth and storage requirements
 - c. Automatic dynamic Frames per Second to lower bandwidth and storage requirements
- d. Transmission
 - 1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
 - 2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.
- e. Image
 - 1. The camera shall incorporate Automatic and Manual White Balance.
 - 2. The camera shall incorporate an electronic shutter operating in the range of 1/66500 s to 1 s.
 - 3. The camera shall incorporate capture mode with the following settings:
 - a. 25/30 fps (WDR-Forensic Capture) (50/60 Hz)
 - b. 50/60 fps (no WDR-Forensic Capture) (50/60 Hz)

4. The camera shall incorporate Wide Dynamic Range - Forensic Capture functionality providing up to 120dB dynamic range.
 5. The camera shall support manually defined values for:
 - a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
 6. The camera shall incorporate a function for optimization of low light behavior.
 7. The camera shall allow for rotation of the image in steps of 90°.
- f. IR Illumination
1. The camera shall be equipped with built-in IR LEDs with adjustable illumination intensity.
 - a. The IR LEDs shall have a range of up to 30 m (100 ft).
 - b. The IR LEDs shall emit light with a wavelength of 850 nm.
- g. User Interface
1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as Verisign, Inc.
 2. Language Specification
 - a. The camera shall provide a function for altering the language of the user interface, and shall include support for at least 10 different languages.
 3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.
 - b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- h. PTZ functionality
1. The camera shall:
 - a. Provide Digital PTZ functionality.
- i. Event functionality
1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection
 - b. Live Stream Accessed
 - c. Day/Night Mode
 - d. Camera tampering
 - e. Manual Trigger/Virtual Inputs

- f. PTZ functionality
 - g. Embedded third party applications
 - h. Edge storage disruption detection
- 2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP, SNMP trap or email
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email
 - d. Send SNMP trap message
 - e. Activate/Deactivate IR Illumination
 - f. Recording to local storage and/or network attached storage
 - g. PTZ control functionality
 - h. WDR mode
- 3. The camera shall provide memory for pre & post alarm recordings.
- j. Edge storage
 - 1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras microSD-card slot
 - b. Network attached storage, located on the local network
 - 2. The camera shall be able to detect and notify Edge storage disruptions.
- k. Protocol
 - 1. The camera shall incorporate support for at least IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, SSH, NTP, CIFS/SMB, Bonjour.
 - 2. The SMTP implementation shall include support for SMTP authentication.
- l. Text overlay
 - 1. The camera shall:
 - a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
 - b. Provide the ability to apply privacy masks to the image.
 - c. Allow for the overlay of a graphical image, such as a logotype, into the image.
- m. Security
 - 1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
 - 2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
 - 3. The camera shall support IEEE 802.1X authentication.
 - 4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
 - 5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.

n. API support

1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
2. The camera shall support relevant ONVIF profiles as defined by the ONVIF Organization.

o. Embedded applications

1. The camera shall provide a platform allowing the upload of third party applications into the camera.

p. Installation and maintenance

1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.
6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.
7. The camera shall provide Remote zoom and Remote focus functionality.

q. Access log

1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.
2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.

r. Camera diagnostics

1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
3. The camera shall send a notification when the unit has re-booted and all services are initialized.

s. Hardware interfaces

1. Network interface

- a. The camera shall be equipped with one 10BASE-T/100BASE-TX PoE Fast Ethernet-port, using a standard connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).
 - t. Enclosure
 - 3. The camera shall:
 - a. Be manufactured with an IP66- and NEMA 4X-rated, IK10 impact-resistant casing.
 - b. Be fitted with a dehumidifying membrane.
 - c. Providing encapsulated electronics and captive screws.
 - u. Power
 - 1. Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3
 - a. Max: 10.8 W
 - b. Typical 7.3 W
 - v. Environmental
 - 1. Operate in a temperature range of -30 °C to +50 °C (-22 °F to 122 °F).
 - 2. Operate in a humidity range of 10–100% RH (condensing).
- D. Fixed mini dome 720p network camera
- 1. The fixed mini dome network camera shall meet or exceed the following design specifications:
 - a. The camera shall operate on an open source; Linux-based platform, and including a built-in web server.
 - b. The camera shall be equipped with a progressive scan megapixel sensor.
 - c. The camera shall provide local video storage utilizing a microSD/microSDHC/microSDXC memory card expansion.
 - d. The camera shall be manufactured with an IP42 water- and dust-resistant, IK08 impact-resistant polycarbonate/ABS casing.
 - e. The camera shall provide a manual 3-axis (pan/tilt/rotation) positioning to allow adjustment for optimum camera rotation and placement.
 - f. The camera shall provide the following camera angle adjustment:
 - 1. Pan $\pm 177^\circ$
 - 2. Tilt $\pm 76^\circ$
 - 3. Rotation $\pm 176^\circ$
 - g. The camera shall provide options for clear and smoked lower dome.
 - 2. The fixed mini dome network camera shall meet or exceed the following performance specifications:
 - a. Illumination
 - 1. The camera shall meet or exceed the following illumination specifications:
 - a. 0.25 lux in color
 - b. Resolution
 - 1. The camera shall be designed to provide at least two video streams in HDTV 720p (1280x720) at up to 30 frames per second (60Hz mode) or 25 frames per second (50Hz mode) using H.264 or Motion JPEG.

2. The camera shall support video resolutions including:
 - a. 1280x720 (HDTV 720p)
 - b. 320x240
 3. The camera shall provide both landscape format (4:3 and 16:9 aspect ratio) as well as corridor format (3:4 and 9:16 aspect ratio).
- c. Encoding
1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 25/30 frames per second in all resolutions.
 - b. Baseline Profile H.264 encoding with motion estimation in up to 25/30 frames per second.
 - c. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 25/30 frames per second.
 - d. Support High Profile H.264 encoding with motion estimation up to 25/30 frames per second.
 - e. Support H.264 with automatic scene adaptive bitrate control in up to 25/30 frames per second.
 2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
 3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate spikes the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
 4. The camera shall provide configurable compression levels.
 5. Support standard baseline profile H.264 with motion estimation.
 6. Support motion estimation in H.264/MPEG-4 Part 10/AVC.
 7. The camera shall have Zipstream technology, an H.264 implementation that supports scene adaptive bitrate control with the following capabilities to lower bandwidth and storage.
 - a. Automatic dynamic Region of Interest to reduce bitrate in unprioritized regions in order to lowering bandwidth and storage requirements.
 - b. Automatic dynamic Group of Pictures to lower bandwidth and storage requirements
 - c. Automatic dynamic Frames per Second to lower bandwidth and storage requirements
- d. Transmission
1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
 2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.
- e. Image

1. The camera shall incorporate Automatic and Manual White Balance.
 2. The camera shall incorporate an electronic shutter operating in the range of 1/32500 s to 1/5 s.
 3. The camera shall incorporate Wide Dynamic Range functionality.
 4. The camera shall provide backlight compensation functionality.
 5. The camera shall support manually defined values for:
 - a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
 6. The camera shall allow for rotation of the image in steps of 90°.
- f. User Interface
1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as Verisign, Inc.
 2. Language Specification
 - a. The camera shall provide a function for altering the language of the user interface, and shall include support for at least 10 different languages.
 3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.
 - b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- g. Event functionality
1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection
 - b. Live Stream Accessed
 - c. Camera tampering
 - d. Manual Trigger/Virtual Inputs
 - e. Embedded third party applications
 - f. Edge storage disruption detection
 2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP, SNMP trap or email
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email

- d. Recording to local storage and/or network attached storage
 - e. Overlay text
- 3. The camera shall provide memory for pre & post alarm recordings.
- h. Edge storage
 - 1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras SD-card slot
 - b. Network attached storage, located on the local network
 - 2. The camera shall be able to detect and notify Edge storage disruptions.
- i. Protocol
 - 1. The camera shall incorporate support for at least IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, SSH, NTP, CIFS/SMB, Bonjour.
 - 2. The SMTP implementation shall include support for SMTP authentication.
- j. Text overlay
 - 1. The camera shall:
 - a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
 - b. Provide the ability to apply privacy masks to the image.
 - c. Allow for the overlay of a graphical image, such as a logotype, into the image.
- k. Security
 - 1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
 - 2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
 - 3. The camera shall support IEEE 802.1X authentication.
 - 4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
 - 5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.
- l. API support
 - 1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
 - 2. The camera shall support relevant ONVIF profiles as defined by the ONVIF Organization.
- m. Embedded applications
 - 1. The camera shall provide a platform allowing the upload of third party applications into the camera.
- n. Installation and maintenance

1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
 2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
 3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
 4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
 5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.
 6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.
- o. Access log
1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.
 2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.
- p. Camera diagnostics
1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
 2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
 3. The camera shall send a notification when the unit has re-booted and all services are initialized.
- q. Hardware interfaces
1. Network interface
 - a. The camera shall be equipped with one 10BASE-T/100BASE-TX PoE Fast Ethernet-port, using a standard male RJ45 connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).
- r. Enclosure
4. The camera shall:
 - a. Be manufactured with an IP42 water- and dust-resistant, IK08 impact-resistant polycarbonate/ABS casing
 - b. Provide encapsulated electronics.
- s. Power
1. Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 1
 - a. Typical 2.5 W
 - b. Max 2.9 W

t. Environmental

1. Operate in a temperature range of 0 °C to +45 °C (+32 °F to 113 °F).
2. Operate in a humidity range of 15–85% RH (non-condensing).
 - a.

E. 1080p PTZ network camera

1. The network camera shall meet or exceed the following design specifications:
 - a. The camera shall operate on an open source; Linux-based platform, and including a built-in web server.
 - b. The camera shall provide a removable IR-cut filter, providing day/night functionality.
 - c. The camera shall provide local video storage utilizing a microSD/microSDHC/microSDXC UHS-I memory card expansion.
 - d. The camera shall be manufactured with an IP66, NEMA 4X and IK09-rated repaintable plastic casing.
 - e. The camera shall provide options for clear and smoked lower dome.
2. The network camera shall meet or exceed the following performance specifications:
 - a. Illumination
 1. The camera shall meet or exceed the following illumination specifications:
 - a. 0.45 lux at 30 IRE F1.6 (Color)
 - b. 0.01 lux at 30 IRE F1.6 (B/W)
 - c. 0.55 lux at 50 IRE F1.6 (Color)
 - d. 0.01 lux at 50 IRE F1.6 (B/W)
 - b. Resolution
 1. The camera shall be designed to provide video streams in HDTV 1080p (1920x1080) at up to 30 frames per second (60Hz mode) or 25 frames per second (50Hz mode) using H.264 or Motion JPEG.
 2. The camera shall support video resolutions including:
 - a. 1920x1080 (HDTV 1080p)
 - b. 1280x720 (HDTV 720p)
 - c. Encoding
 1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 25/30 frames per second in all resolutions.
 - b. Baseline Profile H.264 encoding with motion estimation in up to 25/30 frames per second.
 - c. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 25/30 frames per second.
 - d. Support High Profile H.264 encoding with motion estimation up to 25/30 frames per second.
 - e. Support H.264 with automatic scene adaptive bitrate control in up to 25/30 frames per second.

2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
 3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate spikes the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
 4. The camera shall provide configurable compression levels.
 5. Support standard baseline profile H.264 with motion estimation.
 6. Support motion estimation in H.264/MPEG-4 Part 10/AVC.
 7. The camera shall have Zipstream technology, an H.264 implementation that supports scene adaptive bitrate control with the following capabilities to lower bandwidth and storage.
 - a. Automatic dynamic Region of Interest to reduce bitrate in unprioritized regions in order to lowering bandwidth and storage requirements.
 - b. Automatic dynamic Group of Pictures to lower bandwidth and storage requirements
 - c. Automatic dynamic Frames per Second to lower bandwidth and storage requirements.
- d. Transmission
1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
 2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.
- e. Image
1. The camera shall incorporate Automatic and Manual White Balance.
 2. The camera shall incorporate an electronic shutter operating in the range of 1/66500s to 2s.
 3. The camera shall incorporate Wide Dynamic Range - Forensic Capture functionality.
 4. The camera shall support manually defined values for:
 - a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
 5. The camera shall incorporate a function for optimization of low light behavior.
- f. Audio
1. The camera shall support two-way full duplex audio:
 2. Input sources
 - a. External microphone (balanced/unbalanced)
 - b. External line device
 3. Output sources

- a. External line device
- 4. Encoding
 - a. The camera shall support:
 - 1. AAC LC at 8/16/32 kHz
 - 2. G.711 PCM at 8 kHz
 - 3. G.726 ADPCM 8 kHz
- g. User Interface
 - 1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as Verisign, Inc.
 - 2. Language Specification
 - a. The camera shall provide a function for altering the language of the user interface, and shall include support for at least 10 different languages.
 - 3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.
 - b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- h. PTZ functionality
 - 1. The camera shall:
 - a. Be equipped with accurate pan and tilt functionality
 - 1. Pan: 360°
 - 2. Tilt: 90°
 - b. Provide pan and tilt speed in a range of:
 - 1. 1.8° - 150°/sec
 - 2. 1.8° - 150°/sec
 - c. Provide optical and digital zoom functionality:
 - 1. Optical zoom: 10x
 - 2. Digital zoom: 12x
 - d. Provide preset positions functionality.
 - e. Provide On-screen directional indicator (OSDI) functionality.
- i. Event functionality
 - 1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection

- b. Audio Detection
 - c. Live Stream Accessed
 - d. Camera tampering
 - e. Manual Trigger/Virtual Inputs
 - f. PTZ functionality
 - g. External input
 - h. Embedded third party applications
 - i. Edge storage disruption detection
- 2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP and SNMP trap
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email
 - d. Send SNMP trap message
 - e. Recording to local storage and/or network attached storage
 - f. Activating external output
 - g. Play audio clip
 - h. PTZ control functionality
 - i. WDR mode
- 3. The camera shall provide memory for pre & post alarm recordings.
- j. Edge storage
 - 1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras SD-card slot
 - b. Network attached storage, located on the local network
 - 2. The camera shall incorporate encryption functionality for the SD card.
 - 3. The camera shall be able to detect and notify Edge storage disruptions.
- k. Protocol
 - 1. The camera shall incorporate support for at least IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH
 - 2. The SMTP implementation shall include support for SMTP authentication.
- l. Text overlay
 - 1. The camera shall:
 - a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
 - b. Provide the ability to manually set up and configure up to 20 3D privacy masks to the image.
 - c. Allow for the overlay of a graphical image, such as a logotype, into the image.
- m. Security

1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
 2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
 3. The camera shall support IEEE 802.1X authentication.
 4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
 5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.
- n. API support
1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
 2. The camera shall conform to ONVIF profile S as defined by the ONVIF Organization.
 3. The camera shall conform to ONVIF profile G as defined by the ONVIF Organization.
 - a. For ONVIF profile specifications, see www.onvif.org/
- o. Embedded applications
1. The camera shall support the ACAP platform allowing the upload of third party applications into the camera.
- p. Installation and maintenance
1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
 2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
 3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
 4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
 5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.
 6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.
- q. Access log
1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.
 2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.

r. Camera diagnostics

1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
3. The camera shall send a notification when the unit has re-booted and all services are initialized.

s. Hardware interfaces

1. Network interface

- a. The camera shall be equipped with one 100BASE-TX Fast Ethernet-port, using a standard RJ45 connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).

2. Inputs/Outputs

- a. The camera shall be equipped with four configurable I/O ports, accessible via a removable terminal block. These inputs/outputs shall be configurable to respond to normally open (NO) or normally closed (NC) dry contacts. The output shall be able to provide 12 V DC, 50 mA

3. Audio

- a. The camera shall be equipped with one 3.5 mm jack for line/mic input and one 3.5 mm jack for line output.

4. Power

- a. The camera shall be equipped with a removable terminal block providing connectivity for external power.

t. Enclosure

5. The camera shall:

- a. Be manufactured with an IP66, NEMA 4X and IK09-rated repaintable plastic casing, polycarbonate (PC) dome

u. Power

1. Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3

- a. Max: 12.95 W
- b. Typical: 6.6 W

2. 20 – 28 V DC

- a. Max: 13 W
- b. Typical: 6.3

v. Environmental

1. The camera shall:

- a. Operate in a temperature range of -20 °C to 50 °C (-4 °F to 122 °F)
- b. Operate in a humidity range of 15-100% RH (condensing)

F. PTZ dome 720p network camera

1. The PTZ dome network camera shall meet or exceed the following design specifications:

- a. The camera shall operate on an open source; Linux-based platform, and including a built-in web server.
 - b. The camera shall be equipped with an IR-sensitive progressive scan megapixel sensor.
 - c. The camera shall provide a removable IR-cut filter, providing day/night functionality.
 - d. The camera shall be equipped with a varifocal lens with auto-iris and autofocus.
 - e. The camera shall provide local video storage utilizing a SDHC/SDXC UHS-I memory card expansion.
 - f. The camera shall be manufactured with an IP66-, IK10- and NEMA 4X-rated metal casing (aluminum).
 - g. The camera shall be manufactured with a repaintable metal casing.
2. The PTZ dome network camera shall meet or exceed the following performance specifications:
- a. Illumination
 1. The camera shall meet or exceed the following illumination specifications:
 - a. 0.2 lux at 30 IRE F1.6 (color)
 - b. 0.01 lux at 30 IRE F1.6 (B/W)
 - c. 0.25 lux at 50 IRE F1.6 (color)
 - d. 0.02 lux at 50 IRE F1.6 (B/W)
 - b. Resolution
 1. The camera shall be designed to provide at least two video streams in HDTV 720p (1280x720) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG.
 2. The camera shall support video resolutions including:
 - a. 1280x720 (HDTV 720p)
 - b. 800x450
 - c. 480x270
 - d. 320x180
 - c. Encoding
 1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 50/60 frames per second.
 - b. Baseline Profile H.264 encoding with motion estimation in up to 50/60 frames per second.
 - c. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 50/60 frames per second.
 - d. High Profile H.264 encoding with motion estimation up to 50/60 frames per second.
 - e. H.264 with automatic scene adaptive bitrate control.
 2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
 3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate spikes the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
 4. The camera shall provide configurable compression levels.

5. Support standard baseline profile H.264 with motion estimation.
6. Support motion estimation in H.264/MPEG-4 Part 10/AVC.
7. The camera shall have Zipstream technology, an H.264 implementation that supports scene adaptive bitrate control with the following capabilities to lower bandwidth and storage.
 - a. Automatic dynamic Region of Interest to reduce bitrate in unprioritized regions in order to lowering bandwidth and storage requirements.
 - b. Automatic dynamic Group of Pictures to lower bandwidth and storage requirements
 - c. Automatic dynamic Frames per Second to lower bandwidth and storage requirements
- d. Transmission
 1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
 2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.
- e. Image
 1. The camera shall incorporate Automatic and Manual White Balance.
 2. The camera shall incorporate an electronic shutter operating in the range of 1/45500 to 2 s.
 3. The camera shall incorporate Wide Dynamic Range - Forensic Capture functionality providing up to 120dB dynamic range.
 4. The camera shall provide automatic backlight compensation functionality.
 5. The camera shall support manually defined values for:
 - a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
 6. The camera shall incorporate a function for optimization of low light behavior.
- f. User Interface
 1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as Verisign, Inc.
 2. Language Specification
 - a. The camera shall provide a function for altering the language of the user interface, and shall include support for at least 10 different languages.

3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.
 - b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- g. PTZ functionality
 1. The camera shall:
 - a. Provide more than 255 manually set preset positions.
 - b. Provide a guard tour functionality which allows the dome to automatically move between selected presets using an individual speed and viewing time for each preset.
 - c. Be able to record a custom PTZ tour, operated using an input device such as a joystick, mouse or keyboard, and then use and recall this as a guard tour.
 - d. Provide On-screen directional indicator (OSDI) functionality.
 - e. Be equipped with accurate high-speed pan-tilt functionality with 360° endless pan range and a 180° tilt range.
 - f. Provide focus recall functionality in order to manually set a fixed focus in a predefined area.
 - g. Provide pan speed between 0.1° - 350°/sec.
 - h. Provide tilt speed between 0.1° - 350°/sec.
 - i. Provide 23x optical zoom.
 - j. Provide 12x digital zoom.
- h. Event functionality
 1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection
 - b. Day/Night Mode
 - c. Live Stream Accessed
 - d. Manual Trigger/Virtual Inputs
 - e. PTZ functionality
 - f. Embedded third party applications
 - g. Edge storage disruption detection
 - h. Shock Detected
 2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP, SNMP trap or email
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email
 - d. Send SNMP trap message
 - e. Recording to local storage and/or network attached storage
 - f. PTZ control functionality

- g. WDR mode
- h. Overlay Text
- 3. The camera shall provide memory for pre & post alarm recordings.
- i. Edge storage
 - 1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras SD-card slot
 - b. Network attached storage, located on the local network
 - 2. The camera shall be able to detect and notify Edge storage disruptions.
- j. Protocol
 - 1. The camera shall incorporate support for at least IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, SSH, NTP, CIFS/SMB, Bonjour.
 - 2. The SMTP implementation shall include support for SMTP authentication.
- k. Text overlay
 - 1. The camera shall:
 - a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
 - b. Provide the ability to apply up to 20 individual 3D privacy masks to the image.
 - c. Allow for the overlay of a graphical image, such as a logotype, into the image.
- l. Security
 - 1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
 - 2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
 - 3. The camera shall support IEEE 802.1X authentication.
 - 4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
 - 5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.
- m. API support
 - 1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
 - 2. The camera shall support relevant ONVIF profiles as defined by the ONVIF Organization.
- n. Embedded applications
 - 1. The camera shall provide a platform allowing the upload of third party applications into the camera.
- o. Installation and maintenance

1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
 2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
 3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
 4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
 5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.
 6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.
- p. Access log
1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.
 2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.
- q. Camera diagnostics
1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
 2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
 3. The camera shall send a notification when the unit has re-booted and all services are initialized.
- r. Hardware interfaces
1. Network interface
 - a. The camera shall be equipped with one 10BASE-T/100BASE-TX PoE Fast Ethernet-port, using a standard RJ45 connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).
- s. Enclosure
6. The camera shall:
 - a. Be manufactured with an IP66-, IK10- and NEMA 4X-rated metal casing (aluminum).
 - b. Be manufactured with a repaintable metal casing.
- t. Power
1. Power over Ethernet Plus IEEE 802.3at Type 2 Class 4
 - a. Max: 20 W
 - b. Typical: 8 W

u. Environmental

1. Operate in a temperature range of -30 °C to 55 °C (-22 °F to 131 °F).
2. Operate in a humidity range of 10–100% RH (condensing).

G. 1080p PTZ Dome network camera

1. The PTZ Dome network camera shall meet or exceed the following design specifications:
 - a. The camera shall operate on an open source; Linux-based platform, and including a built-in web server.
 - b. The camera shall be equipped with an IR-sensitive progressive scan sensor.
 - c. The camera shall provide a removable IR-cut filter, providing day/night functionality.
 - d. The camera shall be equipped with a lens providing autofocus and auto-iris functionality.
 - e. The camera shall provide local video storage utilizing a SD/SDHC/SDXC memory card expansion.
 - f. The camera shall be manufactured with an IP66-, IP67-, NEMA 4X- and IK10-rated metal casing (aluminum).
 - g. The camera shall provide options for clear and smoked lower dome.
2. The PTZ Dome network camera shall meet or exceed the following performance specifications:
 - a. Illumination
 1. The camera shall meet or exceed the following illumination specifications:
 - a. 0.3 lux at 30 IRE F1.6 (color)
 - b. 0.03 lux at 30 IRE F1.6 (B/W)
 - c. 0.5 lux at 50 IRE F1.6 (color)
 - d. 0.04 lux at 50 IRE F1.6 (B/W)
 - b. Resolution
 1. The camera shall be designed to provide at least two video streams in HDTV 1080p (1920x1080) at up to 30 frames per second (60Hz mode) or 25 frames per second (50Hz mode) using H.264 or Motion JPEG.
 2. The camera shall be designed to provide at least two video streams in HDTV 720p (1280x720) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG.
 3. The camera shall support video resolutions including:
 - a. 1920x1080 (HDTV 1080p)
 - b. 1280x720 (HDTV 720p)
 - c. 320x180
 - c. Encoding
 1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 50/60 frames per second in resolution 1280x720.
 - b. Motion JPEG encoding in a selectable range from 1 up to 25/30 frames per second in resolution 1920x1080.

- c. Baseline Profile H.264 encoding with motion estimation in up to 50/60 frames per second in resolution 1280x720.
 - d. Baseline Profile H.264 encoding with motion estimation in up to 25/30 frames per second in resolution 1920x1080.
 - e. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 50/60 frames per second in resolution 1280x720.
 - f. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 25/30 frames per second in resolution 1920x1080.
 - g. Support High Profile H.264 encoding with motion estimation up to 50/60 frames per second in resolution 1280x720.
 - h. Support High Profile H.264 encoding with motion estimation up to 25/30 frames per second in resolution 1920x1080.
 - i. Support H.264 with automatic scene adaptive bitrate control in up to 50/60 frames per second in resolution 1280x720.
 - j. Support H.264 with automatic scene adaptive bitrate control in up to 25/30 frames per second in resolution 1920x1080.
2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
 3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate spikes the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
 4. The camera shall provide configurable compression levels.
 5. Support standard baseline profile H.264 with motion estimation.
 6. Support motion estimation in H.264/MPEG-4 Part 10/AVC.
 7. The camera shall have Zipstream technology, an H.264 implementation that supports scene adaptive bitrate control with the following capabilities to lower bandwidth and storage.
 - a. Automatic dynamic Region of Interest to reduce bitrate in unprioritized regions in order to lowering bandwidth and storage requirements.
 - b. Automatic dynamic Group of Pictures to lower bandwidth and storage requirements
 - c. Automatic dynamic Frames per Second to lower bandwidth and storage requirements
- d. Transmission
1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
 2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.
- e. Image
1. The camera shall incorporate Automatic and Manual White Balance.
 2. The camera shall incorporate an electronic shutter operating in the range of:

- a. 1/33000 s to 1/3 s (50 Hz)
 - b. 1/33000 s to 1/4 s (60 Hz)
- 3. The camera shall incorporate Wide Dynamic Range - providing up to 120dB dynamic range.
- 4. The camera shall support manually defined values for:
 - a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
- 5. The camera shall incorporate a function for optimization of low light behavior.
- 6. The camera shall incorporate highlight compensation functionality.
- f. User Interface
 - 1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks shall be signed by an organization providing digital trust services.
 - 2. Language Specification
 - a. The camera shall provide a function for altering the language of the user interface, and shall include support for at least 10 different languages.
 - 3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.
 - b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- g. PTZ functionality
 - 1. The camera shall:
 - a. Provide more than 255 manually set preset positions.
 - b. Provide e-flip functionality, which will automatically rotate the image 180° electronically when following a moving object passing under the camera.
 - c. Provide a guard tour functionality which allows the dome to automatically move between selected presets using an individual speed and viewing time for each preset.
 - d. Be able to record a custom PTZ tour, operated using an input device such as a joystick, mouse or keyboard, and then use and recall this as a guard tour.
 - e. Be able to detect and automatically follow moving objects in the camera's field of view.
 - f. Provide On-screen directional indicator (OSDI) functionality.
 - g. Be equipped with accurate high-speed pan-tilt functionality with 360° endless pan range and a 180° tilt range.

- h. Provide pan and tilt speed between 0.05° - 450°/sec.
 - i. Provide 32x optical zoom.
 - j. Provide 12x digital zoom.
 - k. Provide adjustable zoom speed.
- h. Event functionality
1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection
 - b. Live Stream Accessed
 - c. Manual Trigger/Virtual Inputs
 - d. Fan malfunctioning
 - e. Casing Open
 - f. Heater malfunctioning
 - g. Temperature
 - h. PTZ functionality
 - i. Embedded third party applications
 - j. Edge storage disruption detection
 - k. Shock Detected
 2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP, SNMP trap or email
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email
 - d. Recording to local storage and/or network attached storage
 - e. Day/Night Vision Mode
 - f. PTZ control functionality
 - g. Overlay Text
 3. The camera shall provide memory for pre & post alarm recordings.
- i. Edge storage
1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras SD-card slot
 - b. Network attached storage, located on the local network
 2. The camera shall be able to detect and notify Edge storage disruptions.
- j. Protocol
1. The camera shall incorporate support for at least IPv4, IPv6, USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, SFTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, NTCIP, LLDP.
 2. The SMTP implementation shall include support for SMTP authentication.
- k. Text overlay
1. The camera shall:

- a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
- b. Provide the ability to apply up to 32 3D privacy masks to the image.
- c. Allow for the overlay of a graphical image, such as a logotype, into the image.

l. Security

- 1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
- 2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
- 3. The camera shall support IEEE 802.1X authentication.
- 4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
- 5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.

m. API support

- 1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
- 2. The camera shall support relevant ONVIF profiles as defined by the ONVIF Organization.

n. Embedded applications

- 1. The camera shall provide a platform allowing the upload of third party applications into the camera.

o. Installation and maintenance

- 1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
- 2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
- 3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
- 4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
- 5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.
- 6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.

p. Access log

- 1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.

2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.
- q. Camera diagnostics
 1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
 2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
 3. The camera shall send a notification when the unit has re-booted and all services are initialized.
- r. Hardware interfaces
 1. Network interface
 - a. The camera shall be equipped with one 10BASE-T/100BASE-TX PoE Fast Ethernet-port, using a standard RJ45 connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).
- s. Enclosure
 7. The camera shall:
 - a. Be manufactured with an IP66-, IP67-, NEMA 4X- and IK10-rated metal casing (aluminum).
 2. The camera enclosure shall include the following:
 - a. Sunshield
 - b. Temperature sensors
 - c. Heaters
 - d. Fans
- t. Power
 1. 100-240 VAC / 50-60 Hz, max 60 W – provided to the camera through the network cable by a separate injector, supplied with the camera.
- u. Environmental
 1. Operate in a temperature range of:
 - a. 30 W midspan -20 °C to 50 °C (-4 °F to 122 °F)
 - b. 60 W midspan -50 °C to 50 °C (-58 °F to 122 °F)
 - c. Maximum temperature (intermittent): 60 °C (140 °F)
 2. The camera shall be equipped with Arctic Temperature Control, allowing camera start-up at temperatures down to -40°C (-40°F).
 3. Operate in a humidity range of 10–100% RH (condensing).

H. Four Sensor Degree Camera with optional PTZ

1. The PTZ dome network camera shall meet or exceed the following design specifications:
 - a. The camera shall operate on an open source; Linux-based platform, and including a built-in web server.
 - b. The camera shall be equipped with a progressive scan sensor.

- c. The camera shall provide local video storage utilizing a SD/SDHC/SDXC memory card expansion.
 - d. The camera shall be manufactured with an IP66- and NEMA 4X-rated, die-casted aluminum casing.
 - e. The camera shall incorporate 4x HDTV 720p cameras, providing full 360° overview.
 - f. The camera shall be designed to be compatible with any AXIS Q60-E model.
 - g. The camera shall be manufactured with exchangeable and tiltable lenses.
2. The PTZ dome network camera shall meet or exceed the following performance specifications:
- a. Illumination
 - 1. The camera shall meet or exceed the following illumination specifications:
 - a. 0.3 lux, F2.0 (color)
 - b. Resolution
 - 1. The camera shall be designed to provide four video streams in HDTV 720p (1280x720) at up to 30 frames per second (60Hz mode) or 25 frames per second (50Hz mode) using H.264 or Motion JPEG.
 - 2. The camera shall be designed to provide Quad view in up to 1920x1440 resolution.
 - 3. The camera shall support video resolutions including:
 - a. 1920x1440 (Quad view)
 - b. 1920x1080 (Quad view)
 - c. 1440x1080 (Quad view)
 - d. 1280x960 (Quad view)
 - e. 1280x720 (HDTV 720p)
 - c. Encoding
 - 1. The camera shall support the following video encoding algorithms:
 - a. Motion JPEG encoding in a selectable range from 1 up to 25/30 frames per second.
 - b. Baseline Profile H.264 encoding with motion estimation in up to 25/30 frames per second.
 - c. Main Profile H.264 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 25/30 frames per second.
 - d. High Profile H.264 encoding with motion estimation up to 25/30 frames per second.
 - e. H.264 with automatic scene adaptive bitrate control in up to 25/30 frames per second.
 - 2. The camera shall provide independently configured simultaneous H.264 and Motion JPEG streams.
 - 3. The camera shall in H.264 support Variable Bit Rate (VBR) for video quality adapted to scene content. To protect the network from unexpected bit rate spikes the camera shall support Constant Bit Rate (CBR) or Maximum Bit Rate (MBR).
 - 4. The camera shall provide configurable compression levels.
 - 5. Support standard baseline profile H.264 with motion estimation.
 - 6. Support motion estimation in H.264/MPEG-4 Part 10/AVC.

7. The camera shall have Zipstream technology, an H.264 implementation that supports scene adaptive bitrate control with the following capabilities to lower bandwidth and storage.
 - a. Automatic dynamic Region of Interest to reduce bitrate in unprioritized regions in order to lowering bandwidth and storage requirements.
 - b. Automatic dynamic Group of Pictures to lower bandwidth and storage requirements
 - c. Automatic dynamic Frames per Second to lower bandwidth and storage requirements
- d. Transmission
 1. The camera shall allow for video to be transported over:
 - a. HTTP (Unicast)
 - b. HTTPS (Unicast)
 - c. RTP (Unicast & Multicast)
 - d. RTP over RTSP (Unicast)
 - e. RTP over RTSP over HTTP (Unicast)
 2. The camera shall support Quality of Service (QoS) to be able to prioritize traffic.
- e. Image
 1. The camera shall incorporate Automatic and Manual White Balance.
 2. The camera shall incorporate an electronic shutter operating in the range of 1/45500 s to 4 s.
 3. The camera shall provide backlight compensation functionality.
 4. The camera shall support manually defined values for:
 - a. Color level
 - b. Brightness
 - c. Sharpness
 - d. Contrast
 5. The camera shall incorporate a function for optimization of low light behavior.
- f. User Interface
 1. Web server
 - a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.
 - b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as Verisign, Inc.
 2. Language Specification
 - a. The camera shall provide a function for altering the language of the user interface, and shall include support for at least 10 different languages.
 3. IP addresses
 - a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.

- b. The camera shall allow for automatic detection of the camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.
 - c. The camera shall provide support for both IPv4 and IPv6.
- g. Event functionality
 - 1. The camera shall be equipped with an integrated event functionality, which can be triggered by:
 - a. Video Motion Detection
 - b. Live Stream Accessed
 - c. Camera tampering
 - d. Fan Malfunctioning
 - e. Manual Trigger/Virtual Inputs
 - f. Embedded third party applications
 - g. Edge storage disruption detection
 - h. Shock Detected
 - 2. Response to triggers shall include:
 - a. Send notification, using HTTP, HTTPS, TCP, SNMP trap or email
 - b. Send images, using FTP, HTTP, HTTPS, network share or email
 - c. Send video clip, using FTP, HTTP, HTTPS, network share or email
 - d. Send SNMP trap message
 - e. Recording to local storage and/or network attached storage
 - f. Overlay Text
 - 3. The camera shall provide memory for pre & post alarm recordings.
- h. Edge storage
 - 1. The camera shall support continuous and event controlled recording to:
 - a. Local memory added to the cameras SD-card slot
 - b. Network attached storage, located on the local network
 - 2. The camera shall be able to detect and notify Edge storage disruptions.
- i. Protocol
 - 1. The camera shall incorporate support for at least IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, SSH, NTP, CIFS/SMB, Bonjour.
 - 2. The SMTP implementation shall include support for SMTP authentication.
- j. Text overlay
 - 1. The camera shall:
 - a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.
 - b. Provide the ability to apply privacy masks to the image.
 - c. Allow for the overlay of a graphical image, such as a logotype, into the image.
- k. Security

1. The camera shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
2. The camera shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
3. The camera shall support IEEE 802.1X authentication.
4. The camera shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
5. The camera shall restrict access to the built-in web server by usernames and passwords at three different levels.

l. API support

1. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
2. The camera shall support relevant ONVIF profiles as defined by the ONVIF Organization.

m. Embedded applications

1. The camera shall support the ACAP platform allowing the upload of third party applications into the camera.

n. Installation and maintenance

1. The camera shall be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the cameras' configuration.
2. The camera shall support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.
3. The camera shall allow updates of the software (firmware) over the network, using FTP or HTTP.
4. The camera shall provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.
5. The camera shall accept external time synchronization from an NTP (Network Time Protocol) server.
6. The camera shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.

o. Access log

1. The camera shall provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.
2. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.

p. Camera diagnostics

1. The camera shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.
 2. The camera shall be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.
 3. The camera shall send a notification when the unit has re-booted and all services are initialized.
- q. Hardware interfaces
1. Network interface
 - a. The camera shall be equipped with one 10BASE-T/100BASE-TX/1000BASE-T PoE Fast Ethernet-port, using a standard RJ45 connector and shall support auto negotiation of network speed and transfer mode (full and half duplex).
 - b. The camera shall be equipped with a RJ45 10BASE-T/100BASE-TX connection port for interconnection with Q60-E camera.
 - c. The camera shall be equipped with a RJ45 10BASE-T/100BASE-TX service port.
- r. Enclosure
8. The camera shall:
 - a. Be manufactured with an IP66- and NEMA 4X-rated, die-casted aluminum casing.
 - b. Be manufactured with an polycarbonate dome.
- s. Power
1. 100-240 VAC / 50-60 Hz, max 60 W – provided to the camera through the network cable by a separate injector, supplied with the camera.
 - a. Max: 18 W
 - b. Typical: 8 W
- t. Environmental
1. Operate in a temperature range of -30 °C to 50 °C (-22 °F to 122 °F).
 2. Maximum temperature (intermittent): 60 °C (140 °F)
 3. Operate in a humidity range of 10–100% RH (condensing).

Part 2 Execution

2.01 Installation

1. The Contractors or subcontractors main resources within the project shall carry proper professional certification issued by the manufacturer and verified by a third party organization to confirm sufficient product and technology knowledge.
2. The Contractor shall carefully follow instructions in documentation provided by the manufacturer to ensure all steps have been taken to provide a reliable, easy-to-operate system.
3. All equipment shall be tested and configured in accordance with instructions provided by the manufacturer prior to installation.
4. All firmware found in products shall be the latest and most up-to-date provided by the manufacturer, or of a version as specified by the provider of the Video Management Application (VMA) or Network Video Recorder (NVR).
5. All equipment requiring users to log on using a password shall be configured with user/site-specific password/passwords. No system/product default passwords shall be allowed.
6. A proper installation shall meet NEC (National Electrical Code – US only) per the guidelines of that year's revision. When properly installed equipment meets Low Voltage, Class 2 classification of the NEC.

END OF SECTION

Panasonic IP Cameras – PTZ Dome Camera

PART 1 GENERAL

The CCTV cameras installed at City of Brampton sites are to be manufactured by Panasonic. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.4 of this document.

1.01 SUMMARY

1.02 WARRANTY

- A. Provide manufacturer's standard warranty.

PART 2 PRODUCTS

2.1 MANUFACTURERS

- A. Panasonic Company
- B. Provide Video Surveillance Camera from single source manufacturer

2.2 PANASONIC WV-X6531N PTZ DOME NETWORK CAMERA

A. GENERAL CHARACTERISTICS

1. The PTZ Dome Camera shall deliver H.265 stream and H.264 stream.
2. The PTZ Dome Camera shall produce a resolution of 1,920 x 1,080 pixels (Full HD 1080p) at up to 60 fps with a 16:9 aspect ratio.
3. The PTZ Dome Camera shall produce a resolution of 2,048 x 1,536 pixels at 30fps with a 4:3 aspect ratio.
4. The PTZ Dome Camera shall utilize an approximate 1/2.8-inch type high sensitivity MOS image sensor.
5. The PTZ Dome Camera shall be equipped with 40 times optical zoom.
6. The PTZ Dome Camera shall feature an image stabilization to capture stable images even when installing on the plenty-vibration place.
7. The PTZ Dome Camera shall feature a 144dB wide dynamic range based on Enhanced Super Dynamic and Adaptive Black Stretch technology (ABS).
8. The PTZ Dome Camera shall produce a color image with a minimum illumination of 0.015 lux and a monochrome image with 0.001 lux at F1.6, maximum shutter of 1/30s and High gain mode.

9. The PTZ Dome Camera shall be equipped with a special coated cover for increasing the operational utility of outdoor cameras in rain weather.
10. The PTZ Dome Camera shall generate multiple simultaneous video streams of up to four (4) H.265 (Main profile) or H.264 (High profile) streams and JPEG streams.
11. The PTZ Dome Camera shall be equipped with intelligent auto mode, the technology for shooting license plate and person's face more clearly.
12. The PTZ Dome Camera shall be equipped with GOP control and Smart Facial coding which control an image quality of a stationary area, a moving area and a face, as bitrate reducing technology.
13. The PTZ Dome Camera shall produce encrypted stream.
14. The PTZ Dome Camera shall realize SSL / TLS communication with CA certificate.
15. A user shall be able to view video on a PC using a browser.
16. A user shall be able to view video on a smartphone and tablet using viewer software for iPhone and Android.
17. The PTZ Dome Camera shall offer Video Motion Detection (VMD) with four (4) programmable detection areas, 15 steps sensitivity level and 10 steps detection size.
18. The PTZ Dome Camera shall offer an optional vehicle incident detection function which provides wrong-way detection and stopped vehicle detection.
19. The PTZ Dome Camera shall offer an optional intelligent VMD (i-VMD) function which provides intruder detection, loitering detection, direction detection, scene change detection, object detection and cross line detection.
20. The PTZ Dome Camera shall offer an optional face detection function.
21. The PTZ Dome Camera shall have Fog compensation function.
22. The PTZ Dome Camera shall have High light compensation (HLC) function.
23. The PTZ Dome Camera shall have Super Chroma Compensation (SCC) which realizes a better color reproducibility in the low illumination.
24. The PTZ Dome Camera shall provide up to thirty-two (32) areas of electronic privacy masking.
25. The PTZ Dome Camera shall offer the prioritized stream control which transmits a video stream to a specified client PC or recorder preferentially.

26. The PTZ Dome Camera shall have an SD memory card slot that supports SD, SDHC and SDXC memory card for local storage.
27. The PTZ Dome Camera shall offer full-duplex bi-directional audio communication capability between the camera and monitoring site.
28. The PTZ Dome Camera shall have five (5) alarm sources of terminal input, VMD, command alarm, audio detection alarm and auto track alarm that activate the processes such as SDXC/ SDHC/SD memory recording, E-mail notification, HTTP alarm notification, Indication on browser, FTP image transfer and Panasonic alarm protocol output.
29. The PTZ Dome Camera shall conform to the ONVIF profile S and profile G.

B. CAMERA

1. Image Sensor 1/2.8-inch type MOS image sensor
2. Scanning Mode Progressive
3. Minimum Illumination
 - a. Color 0.015 lux (F1.6, Maximum shutter: Max. 1/30s, Gain: On(11))
 - b. B/W 0.001 lux (F1.6, Maximum shutter: Max. 1/30s, Gain: On(11))
4. Day & Night IR Cut filter Removal
5. Dynamic Range 144 dB typ. (Super Dynamic: On)

C. Lens

1. Focal Length 4.25 ~ 170mm (5/32 ~ 6-11/16 inches)
2. Max. Aperture Ratio 1 : 1.6 (WIDE) ~ 1 : 4.95 (TELE)
3. Angular Field of View
 - a. 16:9 aspect ratio H: 2.1° (TELE) - 65° (WIDE)
V: 1.2° (TELE) - 39° (WIDE)
 - b. 4:3 aspect ratio H: 1.6° (TELE) - 51° (WIDE)
V: 1.2° (TELE) - 39° (WIDE)

D. VIDEO

1. Compression Format H.265, H.264, JPEG
2. Image Resolution
 - a. 16:9 aspect ratio (2 mega pixel mode)
1,920 x 1,080 / 1,280 x 720 / 640 x 360 / 320 x 180 (30/60fps)
 - b. 4:3 aspect ratio (3 mega pixel mode)
2,048 x 1,536 / 1,280 x 960 / 800 x 600 / 640 x 480 / 400 x 300 / 320 x 240 (30fps)
3. H.265 / H.264
 - a. Transmission Mode Constant bitrate, VBR, Frame rate priority, Best effort
 - b. Frame Rate 1 / 3 / 5 / 7.5 / 10 / 12 / 15 / 20 / 30 / 60 fps
 - c. Bit Rate/Client 64 / 128 / 256 / 384 / 512 / 768 / 1,024 / 1,536 / 2,048 / 3,072 / 4,096 / 6,144 / 8,192 / 10,240 / 12,288 / 14,336 / 16,384 / 20,480 / 24,576 / 30,720 / 40,960 kbps
 - d. Image Quality
 - i. Constant bit rate Motion priority / Normal / Quality priority
 - ii. Best effort Motion priority / Normal / Quality priority

- iii. VBR 10 steps
 - e. Transmission type Unicast, Multicast
- 4. JPEG
 - a. Image quality 10 steps
 - b. Transmission type Pull, Push
- E. Audio
 - a. Audio Compression G.726 (ADPCM) 32kbps / 16kbps, G.711 64kbps, AAC-LC 64kbps / 96kbps / 128kbps
 - b. Audio Mode OFF / Mic input / Audio output / Interactive (Half duplex) / Interactive (Full duplex)
- F. OPERATION
 - 1. Super Dynamic On / Off
The level can be set in the range of 0 to 31.
 - 2. Intelligent Auto On / Off
 - 3. Adaptive Black Stretch The level can be set in the range of 0 to 255.
 - 4. Fog compensation On / Off (Only when Intelligent Auto is off.)
 - 5. Black light compensation
High light compensation BLC (Black light compensation) / HLC (High light compensation) / Off
(Only when Super dynamic and Intelligent Auto is off)
 - 6. Maximum shutter Off(1/30) to 1/10000
*1/30 Fix to 2/100 Fix is available during 30 fps mode only. *2/120 Fix is available during 60 fps mode only.
 - 7. Day & Night On / Off / Auto1 (Normal) / Auto2 (IR Light) / Auto3 (SCC)
 - 8. Digital Noise Reduction The level can be set in the range of 0 to 255.
 - 9. Video Motion Detection On / Off, 4 areas, Sensitivity:15 steps, Detection size:10 steps
 - 10. Privacy Zone On / Off, Up to 32 zones
 - 11. Camera Title (OSD) Up to 20 characters
 - 12. Zoom Ratio 40x
 - 13. Digital zoom 16x
 - 14. Panning Range 360-degrees endless
 - 15. Panning Speed
 - a. Manual Approx. 0.065°/s to 120°/s, Up to 256 steps (depending on the controller)
 - b. Preset Up to approx. 300°/s
 - 16. Tilting Range -15° to 195°
 - 17. Tilting Speed
 - a. Manual Approx. 0.065°/s to 120°/s, Up to 256 steps
 - b. Preset Up to approx. 300°/s
- G. NETWORK
 - 1. Network Interface 10Base-T / 100Base-TX, RJ-45 connector
 - 2. IP IPv6, IPv4
 - 3. Supported Protocols
 - a. IPv6 TCP/IP, UDP/IP, HTTP, HTTPS, RTP, FTP, SMTP, DNS, NTP, SNMP, DHCPv6, MLD, ICMP, ARP, DiffServ, IEEE 802.1x

- b. IPv4 TCP/IP, UDP/IP, HTTP, HTTPS, RTSP, RTP, RTP/RTCP, FTP, SMTP, DHCP, DNS, DDNS, NTP, SNMP, UPnP, IGMP, ICMP, ARP, DiffServ, IEEE 802.1x
 - 4. Max. User access Up to 14 users
 - 5. Mobile Terminal Compatibility iPad, iPhone, Android™ mobile terminals
- H. INTERFACE**
 - 1. Monitor Output VBS : 1.0 V [p-p] / 75 ohm, NTSC / PAL composite
 - 2. Microphone input / Line input ø3.5 mm stereo mini jack (monaural input)
 - 3. Audio Output ø3.5 mm stereo mini jack (monaural output)
 - 4. External I/O Terminals ALARM IN 1 (DAY/NIGHT IN), ALARM IN 2 (ALARM OUT), ALARM IN 3 (AUX OUT)
 - 5. SD memory card slot 1 slot, SD/SDHC/SDXC
- I. ELECTRICAL**
 - 1. Power Source AC24V, PoE+ (DC54V, Class 4), Tested PoE Injector(60W, DC54V)
 - 2. Power Consumption Approx. 55W (AC 24V), Approx. 25W (PoE+) Approx. 50W (Tested PoE injector)
- J. SAFETY / EMC**
 - 1. Safety UL (UL60950-1), C-UL (CAN/CSA C22.2 No.60950-1), EN60950-1
 - 2. EMC FCC (Part15 Class A), ICES003 Class A, EN55032 Class A,
- K. MECHANICAL**
 - 1. Dimensions(D x H) ø229 mm x 392 mm (ø9-1/32 inches x 15-7/16 inches)
 - 2. Weight Approx. 5.0 kg (11.02 lbs)
 - 3. Construction material
 - a. Main body Aluminum die cast
 - b. Sunshields ABS+PC resin
 - c. Dome Polycarbonate resin
 - 4. Finish
 - a. Main body Natural silver
 - b. Sunshields Natural silver
 - c. Dome Clear
- L. ENVIRONMENTAL**
 - 1. Ingress Resistance IP66, IEC60529 measuring standard compatible, Type 4X(UL50), NEMA 4X compliant
 - 2. Vandal Resistance Compliant with IEC 62262 IK10
 - 3. Operating Temperature -50 °C ~ +60 °C (-58 °F ~ 140 °F, AC24V)
-30 °C ~ +60 °C (-22 °F ~ 140 °F, PoE+)
 - 4. Operating Humidity 10 % ~ 100 % (without condensation)
- M. SOFTWARE OPTIONS**

1. WV-XAE100W Vehicle incident detection
2. WV-SAE100 Face Detection function
3. WV-SAE200 Intelligent video motion detection

Panasonic IP Cameras – Fixed Dome Camera

PART 1 GENERAL

The CCTV cameras installed at City of Brampton sites are to be manufactured by Panasonic. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.4 of this document.

1.01 SUMMARY

1.02 WARRANTY

- B. Provide manufacturer's standard warranty.

PART 2 PRODUCTS

2.3 MANUFACTURERS

- A. Panasonic System Networks Company
- B. Provide Video Surveillance Camera from single source manufacturer

2.4 PANASONIC WV-S2531LN FIXED DOME NETWORK CAMERA

A. GENERAL CHARACTERISTICS

1. The Fixed Dome Camera shall deliver H.265 stream and H.264 stream.
2. The Fixed Dome Camera shall produce a resolution of 1,920 x 1,080 pixels (Full HD 1080p) at up to 60 fps with a 16:9 aspect ratio.
3. The Fixed Dome Camera shall produce a resolution of 2,048 x 1,536 pixels at 30fps with a 4:3 aspect ratio.
4. The Fixed Dome Camera shall utilize an approximate 1/3 type high sensitivity MOS image sensor.
5. The Fixed Dome Camera shall feature a 144dB wide dynamic range based on Enhanced Super Dynamic and Adaptive Black Stretch technology (ABS).
6. The Fixed Dome Camera shall produce a color image with a minimum illumination of 0.012 lux and a monochrome image with 0.006 lux at F1.6, maximum shutter of 1/30s and High gain mode.
7. The Fixed Dome Camera shall offer a built-in IR illumination to produce a clear monochrome image in zero lux conditions with 40m (131feet) irradiation distance.

8. The Fixed Dome Camera shall be equipped a special coated cover for increasing the operational utility of outdoor cameras in rain weather.
9. The Fixed Dome Camera shall generate multiple simultaneous video streams of up to four (4) H.265 (Main profile) or H.264 (High profile) streams and JPEG streams.
10. The Fixed Dome Camera shall be equipped with intelligent auto mode, the technology for shooting license plate and person's face more clearly.
11. The Fixed Dome Camera shall be equipped with GOP control and Smart Facial coding which control an image quality of a stationary area, a moving area and a face, as bitrate reducing technology.
12. The Fixed Dome Camera shall produce encrypted stream.
13. The Fixed Dome Camera shall realize SSL / TLS communication with CA certificate.
14. A user shall be able to view video on a PC using a browser.
15. A user shall be able to view video on a smartphone and tablet using viewer software for iPhone and Android.
16. The Fixed Dome Camera shall offer Video Motion Detection (VMD) with four (4) programmable detection areas, 15 steps sensitivity level and 10 steps detection size.
17. The Fixed Dome Camera shall have Fog compensation function.
18. The Fixed Dome Camera shall have High light compensation (HLC) function.
19. The Fixed Dome Camera shall have Super Chroma Compensation (SCC) which realizes a better color reproducibility in the low illumination.
20. The Fixed Dome Camera shall provide up to eight (8) areas of electronic privacy masking.
21. The Fixed Dome Camera shall offer the prioritized stream control which transmits a video stream to a specified client PC or recorder preferentially.
22. The Fixed Dome Camera shall have a SD memory card slot that supports SD, SDHC and SDXC memory card for local storage.
23. The Fixed Dome Camera shall offer full-duplex bi-directional audio communication capability between the camera and monitoring site.
24. The Fixed Dome Camera shall have four (4) alarm sources of terminal input, VMD, command alarm and audio detection alarm that activate the processes such as SDXC/SDHC/SD memory recording, E-mail notification, HTTP alarm notification, Indication on browser, FTP image transfer and Panasonic alarm protocol output.

25. The Fixed Dome Camera shall conform to the ONVIF standard.

B. CAMERA

1. Image Sensor 1/3 type MOS image sensor
2. Scanning Mode Progressive
3. Minimum Illumination
 - a. Color 0.012 lux (F1.6, Maximum shutter: Max. 1/30s, Gain: On(High))
 - b. B/W 0.0 lux (with IR LED on)
0.006 lux (F1.6, Maximum shutter: Max. 1/30s, Gain: On(High))
4. Day & Night IR Cut filter Removal
5. Dynamic Range 144 dB typ. (Super Dynamic: On)
6. Built-in IR illumination
 - a. Irradiation distance Approx. 40m (131feet)

C. Lens

1. Vari-Focal Length 2.8 ~ 10mm (1/8 ~ 13/32 inches)
2. Max. Aperture Ratio 1 : 1.6 (WIDE) ~ 1 : 3.35 (TELE)
3. Angular Field of View
 - a. 16:9 aspect ratio H: 30° (TELE) - 108° (WIDE)
V: 17° (TELE) - 58° (WIDE)
 - b. 4:3 aspect ratio H: 25° (TELE) - 90° (WIDE)
V: 19° (TELE) - 65° (WIDE)
4. Focus adjustment Auto Back Focus (ABF) / Manual

D. VIDEO

1. Compression Format H.265, H.264, JPEG
2. Image Resolution
 - a. 16:9 aspect ratio (2 mega pixel mode)
1,920 x 1,080 / 1,280 x 720 / 640 x 360 / 320 x 180 (30/60fps)
 - b. 4:3 aspect ratio (3 mega pixel mode)
2,048 x 1,536 / 1,280 x 960 / 800 x 600 / 640 x 480 / 400 x 300 /
320 x 240 (30fps)
3. H.265 / H.264
 - a. Transmission Mode Constant bitrate, VBR, Frame rate priority, Best effort
 - b. Frame Rate 1 / 3 / 5 / 7.5 / 10 / 12 / 15 / 20 / 30 / 60 fps
 - c. Bit Rate/Client 64 / 128 / 256 / 384 / 512 / 768 / 1,024 / 1,536 / 2,048 / 3,072 /
4,096 / 6,144 / 8,192 / 10,240 / 12,288 / 14,336 / 16,384 /
20,480 / 24,576 / 30,720 / 40,960 kbps
 - d. Image Quality
 - i. Constant bit rate Motion priority / Normal / Quality priority
 - ii. Best effort Motion priority / Normal / Quality priority
 - iii. VBR 10 steps
 - e. Transmission type Unicast, Multicast
4. JPEG
 - a. Image quality 10 steps
 - b. Transmission type Pull, Push

E. Audio

- a. Audio Compression G.726 (ADPCM) 32kbps / 16kbps, G.711 64kbps, AAC-LC
- b. Audio Mode OFF / Mic input / Audio output / Interactive (Half duplex) / Interactive (Full duplex)

F. OPERATION

- 1. Super Dynamic On / Off
The level can be set in the range of 0 to 31.
- 2. Intelligent Auto On / Off
- 3. Adaptive Black Stretch The level can be set in the range of 0 to 255.
- 4. Fog compensation On / Off (Only when Intelligent Auto is off.)
- 5. Black light compensation
High light compensation BLC (Black light compensation) / HLC (High light compensation)
/
Off
(Only when Super dynamic and Intelligent Auto is off)
- 6. AGC The level can be set in the range of 0 to 11.
- 7. Maximum shutter Off(1/30) to 1/10000
*1/30 Fix to 2/100 Fix is available during 30 fps mode only.
- 8. Day & Night On / Off / Auto1 (Normal) / Auto2 (IR Light) / Auto3 (SCC)
- 9. Digital Noise Reduction The level can be set in the range of 0 to 255.
- 10. Video Motion Detection On / Off, 4 areas, Sensitivity:15 steps, Detection size:10 steps
- 11. Privacy Zone On / Off, Up to 8 zones
- 12. Camera Title (OSD) Up to 20 characters
- 13. Digital Zoom 3.6x

G. NETWORK

- 1. Network Interface 10Base-T / 100Base-TX, RJ-45 connector
- 2. IP IPv6, IPv4
- 3. Supported Protocols
 - a. IPv6 TCP/IP, UDP/IP, HTTP, HTTPS, RTP, FTP, SMTP, DNS, NTP, SNMP, DHCPv6, MLD, ICMP, ARP, DiffServ
 - b. IPv4 TCP/IP, UDP/IP, HTTP, HTTPS, RTSP, RTP, RTP/RTCP, FTP, SMTP, DHCP, DNS, DDNS, NTP, SNMP, UPnP, IGMP, ICMP, ARP, DiffServ
- 4. Max. User access Up to 14 users
- 5. Mobile Terminal Compatibility iPad, iPhone, Android™ mobile terminals

H. INTERFACE

- 1. Monitor Output VBS : 1.0 V [p-p] / 75 ohm, NTSC / PAL composite, Pin jack
- 2. Microphone input / Line input
ø3.5 mm stereo mini jack
- 3. Audio Output ø3.5 mm stereo mini jack (monaural output)
- 4. External I/O Terminals ALARM IN 1 (DAY/NIGHT IN), ALARM IN 2 (ALARM OUT), ALARM IN 3 (AUX OUT)
- 5. SD memory card slot 1 slot, SD/SDHC/SDXC

I. ELECTRICAL

- | | |
|----------------------|---|
| 1. Power Source | DC 12V/750mA, PoE (DC48V, Class 0) |
| 2. Power Consumption | Approx. 9W (DC 12V), Approx. 9.4W (PoE) |

J. SAFETY / EMC

- | | |
|-----------|---|
| 1. Safety | UL (UL60950-1), C-UL (CAN/CSA C22.2 No.60950-1), CE, IEC60950-1 |
| 2. EMC | FCC (Part15 Class A), ICES003 Class A, EN55032 Class B, EN55024 |

K. MECHANICAL

- | | |
|--------------------------|---|
| 1. Dimensions(D x H) | ø164 mm x 139 mm (ø6-15/32 inches x 5-15/32 inches) |
| 2. Weight | Approx. 1.6 kg (3.53 lbs, When using based bracket) |
| 3. Construction material | |
| a. Main body | Aluminum die cast |
| b. Front cover | Clear polycarbonate resin |
| 4. Finish | |
| a. Main body | Light gray |
| b. Front cover | Clear |

L. ENVIRONMENTAL

- | | |
|--------------------------|---|
| 1. Ingress Resistance | IP66, IEC60529 measuring standard compatible, Type 4X(UL50), NEMA 4X compliant |
| 2. Vandal Resistance | Compliant with IEC 62262 IK10 |
| 3. Operating Temperature | -40 °C ~ +50 °C (-40 °F ~ 122 °F, When IR-LED is on)
-40 °C ~ +60 °C (-40 °F ~ 140 °F, When IR-LED is off) |
| 4. Operating Humidity | 10 % ~ 90 % (without condensation) |

Panasonic IP Cameras – Panoramic Fixed Dome Camera

PART 1 GENERAL

The CCTV cameras installed at City of Brampton sites are to be manufactured by Panasonic. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.4 of this document.

1.01 SUMMARY

1.02 WARRANTY

- C. Provide manufacturer's standard warranty.

PART 2 PRODUCTS

2.1 MANUFACTURERS

- A. Panasonic System Networks Company
- B. Provide Video Surveillance Camera from single source manufacturer

2.2 PANASONIC WV-SFV481 9MP 360-DEGREE OUTDOOR READY NETWORK CAMERA

A. GENERAL CHARACTERISTICS

1. The 360-degree Camera shall produce a resolution of 2,992 x 2,992 pixels at up to 15 fps with a 9MP fisheye mode.
2. The 360-degree Camera shall produce a resolution of 2,048 x 2,048 pixels at up to 30 fps with a 4MP fisheye mode.
3. The 360-degree Camera shall utilize an approximate 1/2-inch high sensitivity MOS image sensor.
4. The 360-degree Camera shall offer Wide Dynamic Range (WDR).
5. The 360-degree Camera shall produce a color image with a minimum illumination of 0.02 lux and a monochrome image with 0.01 lux at F1.9, shutter speed of 16/30s and High gain mode.
6. The 360-degree Camera shall generate multiple simultaneous video streams of JPEG and H.264 high profile.
7. The 360-degree Camera shall be equipped with GOP control and Auto-VIQS as bitrate reducing technology.

8. The 360-degree Camera shall utilize 3D-Digital Noise Reduction (3D-DNR) to remove visual noises in low light conditions.
9. The 360-degree Camera shall offer Video Motion Detection (VMD) with four (4) programmable detection areas, 15 steps sensitivity level and 10 steps detection size.
10. The 360-degree Camera shall offer an optional intelligent VMD (i-VMD) which provides intruder detection, loitering detection, scene change detection, object detection and cross line detection.
11. The 360-degree Camera shall offer an optional business intelligent functionality which provides heat map, people counting and Moving Object Remover (MOR).
12. The 360-degree Camera shall provide Variable Image Quality on Specified area (VIQS) which sets different image qualities to up to eight (8) areas in the full view to reduce bandwidth and storage capacity requirements.
13. The 360-degree Camera shall have Lens Distortion Compensation to compensate the barrel distortion.
14. The 360-degree Camera shall provide up to eight (8) areas of electronic privacy masking.
15. The 360-degree Camera shall offer the prioritized stream control which transmits a video stream to the specified client PC or recorder preferentially.
16. The 360-degree Camera shall have a SD memory card slot that supports SD, SDHC and SDXC memory card for local storage.
17. The 360-degree Camera shall offer full-duplex bi-directional audio communication between the camera and monitoring site.
18. The 360-degree Camera shall conform to the ONVIF standard.

B. CAMERA

- | | |
|-------------------------|---|
| 1. Image Sensor | 1/2 type MOS image sensor |
| 2. Effective Pixels | Approx. 12.4 megapixels |
| 3. Scanning Mode | Progressive |
| 4. Scanning Area | 5.54 mm (H) x 5.54 mm (V) {7/32 inches(H) x 7/32 inches(V)} |
| 5. Minimum Illumination | |
| a. Color | 0.3 lux (F1.9, Shutter speed of 1/30s, Gain: On(High)) |
| b. B/W | 0.2 lux (F1.9, Shutter speed of 1/30s, Gain : On(High)) |

C. Lens

- | | |
|--------------------------|----------------------------------|
| 1. Focal Length | 1.342mm |
| 2. Angular Field of View | Horizontal: 180°, Vertical: 180° |
| 3. Focus adjustment | Auto Back Focus, Manual |

D. VIDEO

1. Compression Format H.264, JPEG
2. Distribution mode 9M Fisheye mode, 4M fisheye mode, Double Panorama mode,
Quad PTZ / Single PTZ mode, 8M fisheye + Double Panorama mode, 4M fisheye + Double panorama mode, 8M fisheye + Quad PTZ mode, 4M fisheye + Quad PTZ mode, Quad streams mode,
Panorama mode, 8M fisheye + Panorama mode, 4M fisheye + Panorama mode
3. H.264
 - a. Transmission Mode Constant bitrate / VBR / Frame rate priority / Best effort / Advanced VBR
 - b. Frame Rate distribution 1 / 3 / 5 / 7.5 / 10 / 12 / 15 / 20 / 30 fps (depending on mode.)
 - c. Bit Rate/Client 64 / 128 / 256 / 384 / 512 / 768 / 1,024 / 1,536 / 2,048 / 3,072 / 4,096 / 6,144 / 8,192 / 10,240 / 12,288 / 14,336 / 16,384 / 20,480 / 24,576 / 30,720 kbps (depending on distribution mode.)
 - d. Transmission type Unicast, Multicast
4. JPEG
 - a. Image quality 10 steps
 - b. Transmission type Pull, Push

E. Audio

- a. Audio Compression G.726 (ADPCM) 32kbps / 16kbps, G.711 64kbps, AAC-LC
- b. Audio Mode Off / Microphone input / Audio output / Interactive (Half duplex) / Interactive (Full duplex)

F. OPERATION

1. Wide Dynamic Range On / Off
2. Adaptive Black Stretch On / Off
3. AGC On (LOW, MID, HIGH) / Off
4. Day & Night On/ Off
5. Digital Noise Reduction High / Low
6. Video Motion Detection 4 areas, Sensitivity:15 steps, Detection size:10 steps
7. Privacy Zone On/Off, up to 8 zones
8. VIQS Up to 8 zones (fisheye mode only)
9. Camera Title (OSD) Up to 20 characters

G. NETWORK

1. Network Interface 10Base-T / 100Base-TX, RJ-45 connector
2. IP IPv6, IPv4
3. Supported Protocols
 - a. IPv6 TCP/IP, UDP/IP, HTTP, HTTPS, RTP, FTP, SMTP, DNS, NTP, SNMP, DHCPv6, MLD, ICMP, ARP
 - b. IPv4 TCP/IP, UDP/IP, HTTP, HTTPS, RTSP, RTP, RTP/RTCP, FTP,

- | | |
|---------------------|---|
| | SMTP, DHCP, DNS, DDNS, NTP, SNMP, UPnP, IGMP, ICMP, ARP |
| 4. Max. User access | Up to 14 users |
| 5. GUI Language | English, Italian, French, German, Spanish, Portuguese, Russian, Chinese, Japanese |
- H. Intelligent function (optional)**
- | | |
|--------------------------|---|
| 1. Intelligent VMD | Intruder detection, Object detection, Cross line detection, Loitering detection, Scene change detection |
| 2. Business intelligence | Heat map, People count, Moving Object Remover (MOR) |
- I. INTERFACE**
- | | |
|---------------------------|--|
| 1. Monitor Output | VBS : 1.0 V [p-p] / 75 ohm, NTSC / PAL composite, ø3.5mm mini jack, for adjustment |
| 2. Microphone | Built-in microphone |
| 3. Audio Output | ø3.5 mm stereo mini jack |
| 4. External I/O Terminals | ALARM IN 1, ALARM IN 2/ALARM OUT, ALARM IN 3/AUX OUT |
| 5. SD memory card slot | 1 slot, SD/SDHC/SDXC |
- J. ELECTRICAL**
- | | |
|----------------------|--|
| 1. Power Source | DC 12V, PoE |
| 2. Power Consumption | Approx. 10.9W (DC 12V), Approx. 9.6W (PoE) |
- K. SAFETY / EMC**
- | | |
|-----------|---|
| 1. Safety | UL (UL60950-1), C-UL (CAN/CSA C22.2 No.60950-1), CE, IEC60950-1 |
| 2. EMC | FCC (Part15 Class A), ICES003 Class A, EN55022 Class B, EN55024 |
- L. MECHANICAL**
- | | |
|--------------------------|---|
| 1. Dimensions (D x H) | ø150 mm x 52.1 mm {ø5-19/32 x 2-3/64 inches} (excluding the base bracket) |
| 2. Weight | Approx. 0.4 kg (0.88 lbs.) |
| 3. Construction material | ABS resin |
| 4. Finish | Sail white |
- M. ENVIRONMENTAL**
- | | |
|--|------------------------------------|
| 1. Operating Temperature | |
| a. Ceiling, Wall, Camera mount bracket | -10 °C ~ +50 °C (14 °F ~ 122 °F) |
| b. Desktop, Tripod | -10 °C ~ +40 °C (14 °F ~ 104 °F) |
| 2. Operating Humidity | 10 % ~ 90 % (without condensation) |
- N. SOFTWARE OPTIONS**
- | | |
|--|--|
| 1. Extension Software for intelligent function | |
|--|--|

END OF SECTION

28 30 00 Security Detection, Alarm and Monitoring

1.0 General

The Security Detection and Alarm Monitoring systems installed at City of Brampton sites are to be manufactured by DSc by Tyco. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.5 of this document.

2.0 Introduction

The purpose of this section is to introduce you to the PC1864 alarm panel and to provide you with detailed information on its specifications and features. The following areas are covered in this section:

- Regulatory requirements
- Model features

3.0 Regulatory Requirements - Canada

ULC

- i. ULC-S545-2002 Standard for Residential Fire Warning System Control Units
- ii. ORD-C1023-1974 Standard for Household Burglar Alarm System Units
- iii. CAN/ULC-S304-2006 Standard for Central & Monitoring Station Burglar Alarm Systems
- iv. CAN/ULC-S559-2004 Standard for Equipment for Fire Signal Receiving Centers and Systems

IC

- v. ICES-003 (CISPR22 Class B) Standard for Interference Causing Equipment, Digital Apparatus
- vi. IC-CS03 Issue 9, Industry Canada Terminal Equipment Technical Specifications

4.0 Technical Requirements

- 3.1 8 on-board zones
- 3.2 Expandable to 64 hardwired zones
- 3.3 Expandable to 64 wireless zones
- 3.4 4 PGM outputs: expandable to 14 (PC5204, PC5208)
- 3.5 Support for template programming
- 3.6 Connect up to 8 supervised keypads
- 3.7 Support for up to 8 partitions
- 3.8 Supports up to 500-event buffer
- 3.9 Supports up to 95 user codes
- 3.10 ANSI/SIA CP-01 compliant
- 3.11 Supports wire free keypads with TR5164-433 transceiver
- 3.12 Compatible with leading edge interactive services supported by DSC

END OF SECTION

28 50 00 Specialized Systems – Intercom Entry Systems

The Intercom Entry Systems installed at City of Brampton sites are to be manufactured by Commend International. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.6 of this document.

1.0 Technical Specifications – ES831/3A

- .1 Fully interoperable with Commend GE 800 / GE300 Intercom Servers
- .2 Keyboard supports ability to connect 12 buttons, with plug for row/column matrix
- .3 Omnidirectional electret microphone for max. 7 m (23 ft) speaking distance
- .4 Loudspeaker utilizes special membrane type for optimal sound quality, sound pressure: 85 dB/1 W/1 m (3.28 ft), 8 Ohm
- .5 Built-in amplifier 2.5 W output power with built-in loudspeaker: 1.5 W
- .6 1 input for floating contacts, max. 1 KOhm (detection of 5 input states)
- .7 1 relay output 30V/1A
- .8 Call indication: multifunctional LED (colours: red, green, blue)
- .9 Frequency range: 200 — 16,000 Hz
- .10 Operating temperature range: -20° C to +70° C (-4° F to 158° F)
- .11 Storage temperature range: -20° C to +70° C (-4° F to 158° F)
- .12 Relative humidity: up to 95 %
- .13 Expansion: pluggable screw terminals - expansion plug for e.g. EB 2E2A
- .14 Cabling: star feed, 2-wire, twisted
- .15 Power Supply: From Intercom Server or optional external power supply enabling greater line length - (12-24 VAC or 15-35 VDC, 500 mA)
- .16 Signaling: 2B + D (2 x 64 kBit/s speech, 16 kBit/s data)
- .17 Dimensions: 875 x 109 x 40 mm (3.45 x 4.29 x 1.58 in)
- .18 Vandal Resistant (EN 62262 IK09) Housing with stainless steel face plate

2.0 Technical Specifications – EF 962H

- .1 IP rating: IP54 (acc. EN 60529)
- .2 Mechanical impact resistance: IK09 (acc. EN 62262)
- .3 Front Panel: stainless steel, 3 mm (0.12 in)
- .4 Microphone: electret condenser microphones polar pattern: omnidirectional
- .5 Loudspeaker: special membrane type for optimal sound quality, 8 ohm
- .6 Sound pressure Level: 85 dB/1 W/1 m (3.28 ft)
- .7 Amplifier:) integrated class-D amplifier with 10 W
- .8 Inputs: 2 inputs for floating contacts (IP: detection of 5 input states)
- .9 Outputs: 2 relay outputs (1 switch-over contact, 1 normally open contact) max. 60 VDC, 2 A, 60 W, expected life: min. 5×10^6 (2 A), 10^7 (1 A)
- .10 Call button: EF 62H: stainless steel button EF 962HM: red mushroom button.
- .11 IP transmission bandwidth: 16 KHz
- .12 SIP Transmission bandwidth: 7 KHz
- .13 Operating Temperature Range: -30 °C to 70 °C (-22 °F to 158 °F)
- .14 Storage Temperature Range: -30 °C to 70 °C (-22 °F to 158 °F)
- .15 Relative Humidity: up to 95%, not condensing
- .16 Connections: pluggable spring clamp terminals, expansion plug e.g. for EB2E2AHE, IP Uplink: shielded RJ45 modular jack
- .17 Power Supply: PoE (Power over Ethernet): IEEE 802.3af power consumption: Class 0 (0.44 to 12.96 W)
- .18 Cabling: minimum Cat5. The maximum line length of Cat. 5 cabling in a LAN is 90 m (295 ft) - e.g. from switch to Intercom station.
- .19 IP Protocols: IPv4, UDP, DHCP, RTP, RTCP, SNMPv2c, SNMPv4

- .20 SIP Protocols; SIP (RFC 3261), SNMPv2, STUN, TFTP, URI (RFC 2396), DTMF Decoding (RFC 2876, RFC 2833), SIP User Agent (UDP RFC 3261), SIP Refer Method (RFC 3515)
- .21 Audio Codecs: G.711 a-Law, G.711 p-Law, G.722
- .22 Data rate: 10/100 MBit/s (Full/Half Duplex) Auto MDIX
- .23 Mounting: Flush or Surface mount with accessory boxes
- .24 Dimensions: front panel (W x H): 110 x 151 mm (4.33 x 5.95 in) depth flush mount: 48 mm (1.89 in) depth surface mount: 84 mm (3.3 in), except for EF 62W: 55 mm (2.2 in)
- .25 Communication Ports: SIP – UDP 5060, RTP – UDP 16384 incoming, UDP 16400 (configurable), TCP 16399 station config (not configurable)
- .26 Compatible Third Party SIP Servers: Cisco, Digium, Avaya/Nortel, Innovaphone, Alcatel, Siemens, 3CX, Starface, Astra/Ericsson, Kamailio, FreeSwitch, ELMPEG, 2N, AVM, SipGate, Vodafone Arcor, blue SIP, Mitel

3.0 Technical Specifications – GE 300 Server

- .1 Intercom Server with five plug-in slots
- .2 Up to 40 subscribers possible
- .3 One AF input (for music or alarm)
- .4 Two inputs for floating contacts
- .5 Two relay outputs: max switching capacity 60W / 62.5 VA, max switching current 2A, max switching voltage 60 VDC/30VAC
- .6 Configuration via Ethernet (Layer 2) or RS-232
- .7 Power Supply: 24 VDC
- .8 Emergency Power Consumption: without cards, 200 mA, maximum 40 VA
- .9 Power Consumption: max 30W, 60W, or 70W depending on settings
- .10 Frequency Response: 50 Hz to 150 kHz (-3dB)

- .11 Total Harmonic Distortion: <0.9%
- .12 Music Input: max 800 mV RMS at 10 kΩ, 16 kHz
- .13 Inputs – IN1, IN2: for floating contacts, max. line resistance = 1.5 kΩ
- .14 Operating temperature range: 0° C to +50° C (32° F to 122° F)
- .15 Storage temperature range: -30° C to +60° C (-22° F to 140° F)
- .16 Relative Humidity: 20 to 80%, not condensing
- .17 Mounting: wall mounting
- .18 Dimensions: 310x210x77.5 mm
- .19 Max Subscribers: 16 – 30W PS, 20 – 60W PS

4.0 Technical Specifications – GE 800 Server

- .1 Compatibility: IP, 2-wire, and 4 wire subscriber stations
- .2 Expandability: up to 25,000 subscriber stations without restrictions, 112 per housing up to 239 housings
- .3 Power Supply: 24VAC 80VA, 24-35VDC, 80W
- .4 Emergency power consumption: 200 mAh, plus load from configured cards
- .5 Frequency range: 50Hz to 16 kHz
- .6 Operating temperature range: 0° C to +50° C (32° F to 122° F)
- .7 Storage temperature range: -30° C to +60° C (-22° F to 140° F)
- .8 Dimensions: 483 x 133 x229 mm
- .9 Relative Humidity: 20 to 80%, not condensing
- .10 Mounting: 19 inch rack mount, 3U

- .11 **Relay outputs:** max switching capacity 60W / 125 VA, max switching current 2A, max switching voltage 60 VDC/40VAC
- .12 Music Input: max 800 mV RMS at 10 k Ω , 16 kHz
- .13 Inputs – IN1, IN2: for floating contacts, max. line resistance = 1.5 k Ω
- .14 Thermal dissipation loss: 45.2W

END OF SECTION

26 33 00 Battery Equipment

1.0 General

The battery backup units installed at City of Brampton sites are to be manufactured by APC by Schneider Electric. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.9 of this document.

2.0 Regulatory Compliance

UL 1449, UL 1778CSA, CSA C22.2 No 107.1, FCC part 15 Class, ICES-003

3.0 Technical Requirements – 1.5kVA Standalone UPS

- .1 Battery power: 1500VA / 750W
- .2 Total Controlled outlets = 4
- .3 LCD display
- .4 Remote reboot capability via single switched outlet
- .5 User replaceable batteries
- .6 Max output power capacity: 1.0 kWatts
- .7 Nominal output voltage: 120VAC
- .8 Output voltage distortion: less than 5%
- .9 Secondary output voltages: 110, 127
- .10 Topology: Line interactive
- .11 Waveform type: Sine wave
- .12 Transfer time: max 10 ms

- 4.0 Technical Requirements – 1.5 kVA Rack Mount UPS
 - 1.0 Battery power: 1500VA / 750W
 - 2.0 Total Controlled outlets = 3
 - 3.0 LCD display
 - 4.0 Remote reboot capability via single switched outlet
 - 5.0 Network management capable via SmartSlot and APC PowerChute Network Monitoring Software
 - 6.0 User replaceable batteries
 - 7.0 Nominal output voltage: 120VAC
 - 8.0 Output voltage distortion: less than 5%
 - 9.0 Secondary output voltages: 110, 127
 - 10.0 Topology: Line interactive
 - 11.0 Waveform type: Sine wave
 - 12.0 Transfer time: max 10 ms
 - 13.0 Output frequency (sync to mains): 50/60Hz +/- 3 Hz

END OF SECTION

27 11 00 Communications Equipment Room Fittings

1.0 General

The communications room fittings installed at City of Brampton sites are to be manufactured by Middle Atlantic. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.10 of this document.

2.0 Technical Specification – Full Height Rack

- 2.1 Standards Compliance: c/UL 2416, ASCE 7-10, RoHS, Greenguard, CSA
- 2.2 Overall dimensions of rack shall be: W x D = 1800 x 702 mm
- 2.3 Useable dimensions of rack shall be: W x D – 1648 x 654 mm
- 2.4 Usable interior width: 483 mm / 19 inches
- 2.5 Four post construction with extra wide pairs of 11 gauge 10-32 threaded rack rail with numbered rack space increments.
- 2.6 c/UL listed load capacity: 2500 lbs.
- 2.7 Static load capacity: 10,000 lbs.
- 2.8 Seismic certified load capacity: 900 lbs., requires WRK-Z4 option
- 2.9 ½ inch, 2/3 inch, 1 inch, 1 ½ inch electrical knockouts on split rear plates top and bottom for cable pass through
- 2.10 Key locked solid rear door included
- 2.11 Black powder coat finish
- 2.12 Required accessories: vented side panels, vented locking doors, roof fan panel kits with high flow i.e. 550 CFM fan kits, rack shelves, horizontal and vertical cable management, horizontal and vertical power distribution units

3.0 Technical Specification – Wall Mount Rack (10U)

- 3.1 Standards Compliance: UL Listing No: E313734, ASCE 7-10, RoHS, Greenguard, CSA
- 3.2 Overall dimensions of 10U rack shall be: H x D – 624 x 594 mm
- 3.3 Useable dimensions of 10U rack shall be: H x D - 444.5 x 508 mm
- 3.4 Useable interior width: 483 mm / 19 inches
- 3.5 Two 11 gauge 10-32 threaded rack rail with numbered rack space increments.
- 3.6 c/UL listed load capacity: 200 lbs.
- 3.7 Static load capacity: 800 lbs.
- 3.8 Seismic certified load capacity: 155 lbs. 2007 & 2010 CBC; 2006, 2009 & 2012 IBC; ASCE 7-05 (2005 Edition) & ASCE 7-10 (2010 Edition) and the 2006 & 2009 editions of NFPA 5000 for use in areas of high seismicity,
- 3.9 ½ inch, 2/3 inch, 1 inch, 1 ½ inch, 2 inch and 3 inch electrical knockouts on split rear plates top and bottom for cable pass through
- 3.10 Locking solid front door
- 3.11 Black powder coat finish
- 3.12 Required accessories: vented side panels, vented locking doors, roof fan panel kits with high flow i.e. 550 CFM fan kits, rack shelves, horizontal and vertical cable management, horizontal and vertical power distribution units

4.0 Technical Specification – Wall Mount Rack (16U)

- 4.1 Standards Compliance: UL Listing No: E313734, ASCE 7-10, RoHS, Greenguard, CSA
- 4.2 Overall dimensions of 16U rack shall be: H x D – 891 x 566 mm
- 4.3 Useable dimensions of 16U rack shall be: H x D - 711 x 508 mm
- 4.4 Useable interior width: 483 mm / 19 inches
- 4.5 Two 11 gauge 10-32 threaded rack rail with numbered rack space increments.
- 4.6 c/UL listed load capacity: 200 lbs.
- 4.7 Static load capacity: 800 lbs.

- 4.8 Seismic certified load capacity: 155 lbs. 2007 & 2010 CBC; 2006, 2009 & 2012 IBC; ASCE 7-05 (2005 Edition) & ASCE 7-10 (2010 Edition) and the 2006 & 2009 editions of NFPA 5000 for use in areas of high seismicity,
- 4.9 ½ inch, 2/3 inch, 1 inch, 1 ½ inch, 2 inch and 3 inch electrical knockouts on split rear plates top and bottom for cable pass through
- 4.10 Locking solid front door
- 4.11 Black powder coat finish
- 4.12 Required accessories: vented side panels, vented locking doors, roof fan panel kits with high flow i.e. 550 CFM fan kits, rack shelves, horizontal and vertical cable management, horizontal and vertical power distribution units

5.0 Technical Specification – Wall Mount Rack (22U)

- 5.1 Standards Compliance: UL Listing No: E313734, ASCE 7-10, RoHS, Greenguard, CSA
- 5.2 Overall dimensions of 22U rack shall be: H x D – 1246 x 566 mm
- 5.3 Useable dimensions of 22U rack shall be: H x D – 1067 x 508 mm
- 5.4 Useable interior width: 483 mm / 19 inches
- 5.5 Two 11 gauge 10-32 threaded rack rail with numbered rack space increments.
- 5.6 c/UL listed load capacity: 300 lbs.
- 5.7 Static load capacity: 1,200 lbs.
- 5.8 Seismic certified load capacity: 155 lbs. 2007 & 2010 CBC; 2006, 2009 & 2012 IBC; ASCE 7-05 (2005 Edition) & ASCE 7-10 (2010 Edition) and the 2006 & 2009 editions of NFPA 5000 for use in areas of high seismicity,
- 5.9 ½ inch, 2/3 inch, 1 inch, 1 ½ inch, 2 inch and 3 inch electrical knockouts on split rear plates top and bottom for cable pass through
- 5.10 Locking front door with plexiglass insert
- 5.11 Black powder coat finish
- 5.12 Required accessories: vented side panels, vented locking doors, roof fan panel kits with high flow i.e. 550 CFM fan kits, rack shelves, horizontal and vertical cable management, horizontal and vertical power distribution units

END OF SECTION

27 20 00 Data Communications

1.0 General

The data communications equipment installed at City of Brampton sites are to be manufactured by Cisco Systems. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.7 of this document.

2.0 Regulatory Compliance

The products specified herein comply with UL (UL 60950), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A.

3.0 Technical Specifications – 10 Port PoE Switch, SG250-10P

- .1 Device Type: Switch, Gigabit, 10 Ports, PoE
- .2 Enclosure Type; Compact, single unit
- .3 Ports: 8 x 10/100/1000, 2 x Gigabit SFP/RJ-45
- .4 Power Over Ethernet Capability: PoE+ (8 ports, 62W)
- .5 Switching Capacity: 20-Gbps
- .6 Forwarding performance (64-byte packets): 14.88-Mpps forwarding performance (64-byte packet size)
- .7 MAC address table size: 8K entries
- .8 Capacity (active VLANs): 256
- .9 Remote management protocol: SNMP, RMON, HTTP, HTTPS, TFTP, Telnet, SSH
- .10 Features: Layer 2 switching, Layer 3 switching, DHCP support, BOOTP support, VLAN support, IGMP snooping, Syslog support, port mirroring, DiffServ support, Weighted Round Robin (WRR) queuing, Broadcast Storm Control, IPv6 support, Multicast Storm Control, Unicast Storm Control, STNP support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree (MSTP), Trivial File Transfer Protocol (TFTP) support, access control list (ACL) support, quality of service (QoS), jumbo frames support, MLD snooping, SNMP, RMON, STNP, Cisco Discovery Protocol, Auto SmartPorts

- .11 Compliant standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3af PoE, IEEE 802.3at PoE, IEEE 802.3az
- .12 RAM: 512 MB
- .13 Flash Memory: 256 MB Flash
- .14 Status Indicators: System, link/speed per port
- .15 Expansion and Connectivity Interfaces: 8 x 10BASE-T/100BASE-TX/1000BASE-T, RJ-45 (PoE+), 2 x Gigabit SFP/RJ-45 (60W PoE PD)
- .16 Power Supply: Power supply, external
- .17 Voltage Required: AC 120/230V (50/60 Hz)
- .18 Width: 11.0 in (280 mm)
- .19 Depth: 6.69 in (170 mm)
- .20 Height: 1.45 in (44 mm)
- .21 Weight: 2.65 lb (1.2 kg)
- .22 Warranty: Limited Lifetime Warranty
- .23 Operating temperature range: 0° C to +50° C (32° F to 122° F)
- .24 Storage temperature range: -20° C to +70° C (-4° F to 158° F)
- .25 Relative Humidity (operations and storage): 10 to 90%, not condensing

4.0 Technical Specifications – 24 Port PoE Switch @ 195W, SC250X-24P

- .1 Device Type: Switch, Gigabit, 24 Ports, PoE/PoE+
- .2 Enclosure Type: Rack mount, 1U
- .3 Ports: 24 x 10/100/1000, 2 x 10 GE copper, 2 x 10 GE SFP+
- .4 Power Over Ethernet Capability: PoE+ (24 ports, 195W)
- .5 Switching Capacity: 128-Gbps

- .6 Forwarding performance (64-byte packets): 95.23-Mpps forwarding performance (64-byte packet size)
- .7 MAC address table size: 8K entries
- .8 Capacity (active VLANs): 256
- .9 Remote management protocol: SNMP, RMON, HTTP, HTTPS, TFTP, Telnet, SSH
- .10 Features: Layer 2 switching, Layer 3 switching, DHCP support, BOOTP support, VLAN support, IGMP snooping, Syslog support, port mirroring, DiffServ support, Weighted Round Robin (WRR) queuing, Broadcast Storm Control, IPv6 support, Multicast Storm Control, Unicast Storm Control, STP support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree (MSTP), Trivial File Transfer Protocol (TFTP) support, access control list (ACL) support, quality of service (QoS), jumbo frames support, MLD snooping, SNMP, RMON, STP, Cisco Discovery Protocol, Auto SmartPorts
- .11 Compliant standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3af PoE, IEEE 802.3at PoE, IEEE 802.3az
- .12 RAM: 512 MB
- .13 Flash Memory: 256 MB Flash
- .14 Status Indicators: System, link/speed per port
- .15 Expansion and Connectivity Interfaces: 24 x 10BASE-T/100BASE-TX/1000BASE-T, RJ-45, PoE, 2 x 10GBASE-T, 2 x SFP+
- .16 Power Supply: Internal
- .17 Voltage Required: AC 120/230V (50/60 Hz)
- .18 Width: 17.3 in (440 mm)
- .19 Depth: 10.12 in (257 mm)
- .20 Height: 1.45 in (44 mm)
- .21 Weight: 8.51 lb (3.86 kg)
- .22 Warranty: Limited Lifetime Warranty
- .23 Operating temperature range: 0° C to +50° C (32° F to 122° F)
- .24 Storage temperature range: -20° C to +70° C (-4° F to 158° F)

- .25 Relative Humidity (operations and storage) : 10 to 90%, not condensing

5.0 Technical Specifications – 24 Port PoE Switch @ 375W, SC350X-24MP

- .1 Device Type: Switch: L3 managed, 24 x 10/100/1000 + 2 x 10GE combo + 2 x 10GE SFP+, rack-mountable, Max PoE
- .2 Enclosure Type: Rack mount, 1U
- .3 Ports: 24 x 10/100/1000 + 2 x 10GE copper/SFP+ combo + 2 x 10GE SFP+
- .4 Power Over Ethernet Capability: PoE, PoE+ and 60W PoE (375W)
- .5 Switching Capacity: 128-Gbps
- .6 Forwarding performance (64-byte packets): 95.23-Mpps forwarding performance (64-byte packet size)
- .7 MAC address table size: 16K entries
- .8 Capacity (active VLANs): 4000
- .9 Remote management protocol: SNMP1, RMON1, RMON2, RMON3, RMON9, Telnet, SNMPv3, SNMPv2c, HTTP, HTTPS, SSH, CLI
- .10 Routing: Static IPv4 /IPv6 routing
- .11 Features: Stacking, flow control, Layer 2 switching, Layer 3 switching, VLAN support, IPv6 support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, access control list (ACL) support, quality of service (QoS), reset button, LACP support, Energy Efficient Ethernet, dynamic VLAN support (GVRP), advanced threat protection, IPv6 first-hop security, static routing, sFlow, RSPAN
- .12 Compliant standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.3ae, IEEE 802.3an, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az
- .12 RAM: 512 MB
- .13 Flash Memory: 256 MB Flash
- .14 Status Indicators: System, Master, Fan, Stack ID, Link/Speed per port

- .15 Expansion and Connectivity Interfaces: 24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 - PoE, 2 x 10GBase-T/SFP+ combo, 2 x SFP+, 1 x console - RJ45
- .16 Power Supply: Internal
- .17 Voltage Required: AC 120/230V (50/60 Hz)
- .18 Width: 17.3 in (440 mm)
- .19 Depth: 13.8 in. (350 mm)
- .20 Height: 1.73 in. (44 mm)
- .21 Weight: 12.54 lb (5.69 kg)
- .22 Warranty: Enhanced limited Lifetime Warranty
- .23 Operating temperature range: 0° C to +50° C (32° F to 122° F)
- .24 Storage temperature range: -20° C to +70° C (-4° F to 158° F)
- .25 Relative Humidity (operations and storage) : 10 to 90%, not condensing

END OF SECTION

27 22 00 Data Communications Hardware

1.0 General

The computers, laptops, workstations, servers, and storage arrays installed at City of Brampton sites are to be manufactured by either Dell or Hewlett Packard.. The system integrator providing the equipment will ensure that all units are in compliance with the general requirements listed in section 2.7 of this document.

2.0 Regulatory Compliance

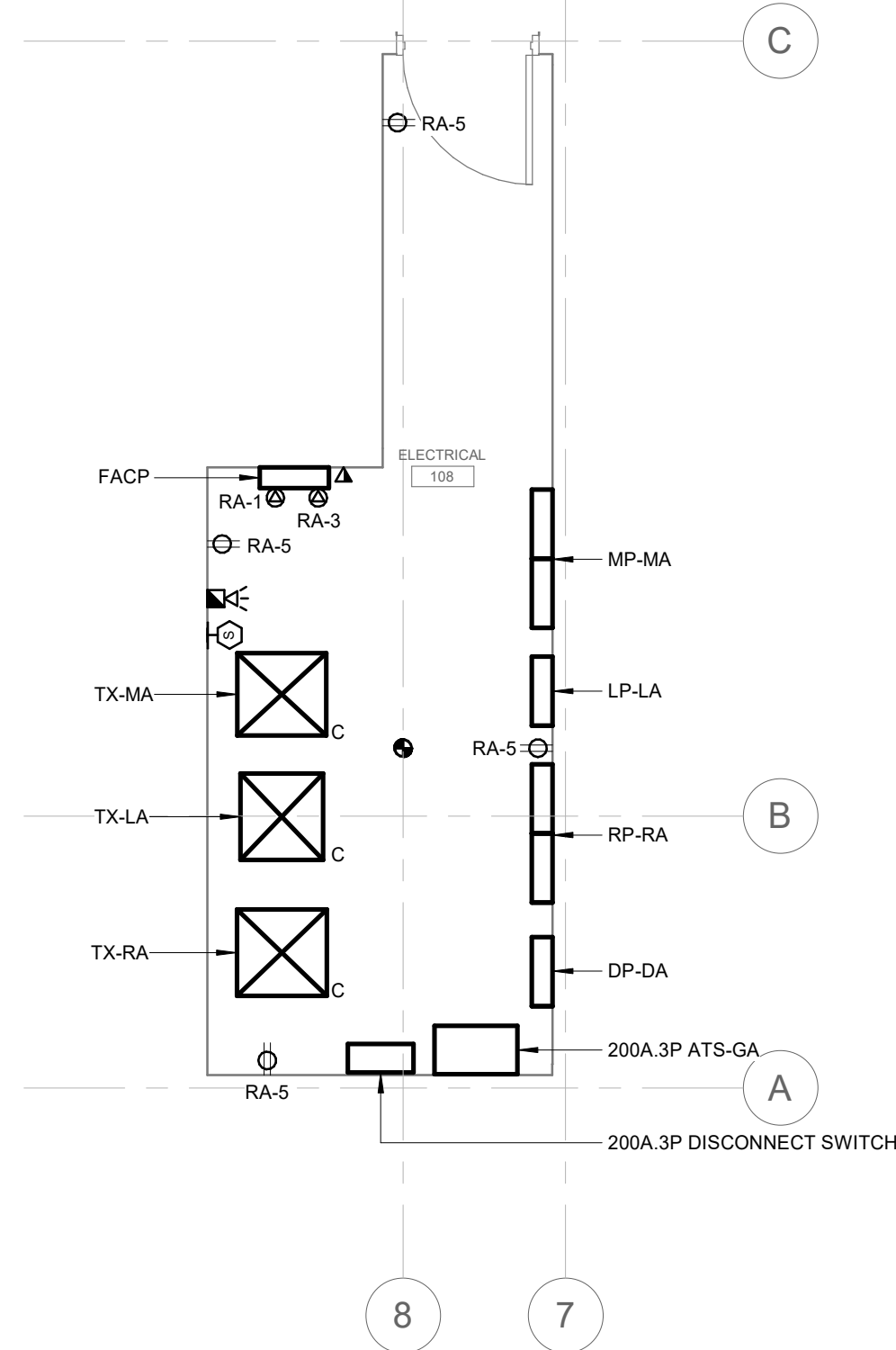
It is the responsibility to the integrator to ensure that all supplied hardware have the required UL, c/UL, CSA and IC certifications where required.

3.0 Technical Requirements

Due to the rapid pace of change of computer technology, formal specifications for each class of device have not been provided. It is the responsibility of the integrator to confirm the compatibility of each laptop, computer, workstation, server, and storage array against manufacturer provider minimum configurations for system performance. Should any deficiencies in system operation due to incorrect or incompatible system configurations be found, it will be the responsibility of the solution provider to correct the deficiencies at their sole expense.

IT ROOM 109 - LAYOUT

SCALE: 1 : 50



- GENERAL NOTES:**
- ALL TRANSFORMERS SHOWN ARE TO BE SUSPENDED FROM CEILING SLAB.

ELECTRICAL ROOM 108 - LAYOUT

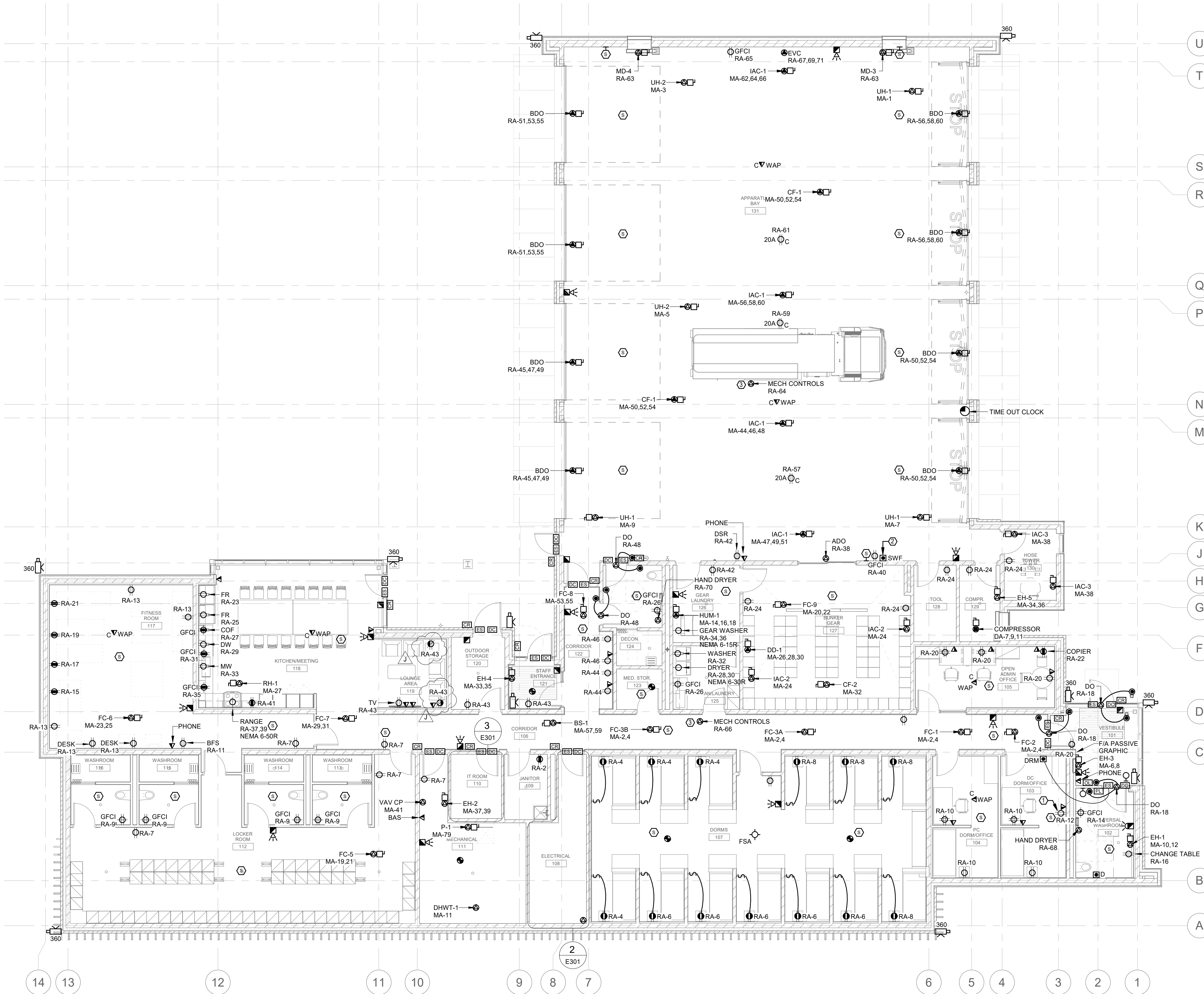
SCALE: 1 : 50

GENERAL NOTES:

- ALL RECEPTACLES AND COMMUNICATION OUTLET BOXES TO BE INSTALLED UNDER DESKS ARE TO BE MOUNTED 775mm ABOVE FINISHED FLOOR AS PER CITY OF BRAMPTON IT SPECIFICATION'S APPENDIX C (SECTION 27 00 00).
- PROVIDE A NEMA 5-15 RECEPTACLE FED FROM PANEL RP-RA (CCT. #62) AND PROTECTED BY A 15A 1P DEDICATED BREAKER TO BE LOCATED ADJACENT TO RADIO EQUIPMENT CABINET. CONFIRM EXACT LOCATION OF CABINET WITH SIGNALLING CONTRACTOR PRIOR TO INSTALLATION.
- PROVIDE 1-2" CONDUIT FROM ELECTRICAL ROOM TO ROOF FOR FUTURE SOLAR PANEL ARRAY. CONFIRM EXACT TERMINATION POINTS OF CONDUIT ON SITE.

KEYNOTES:

- RECEPTACLE TO BE USED FOR WALL MOUNTED DISPLAY THAT MONITORS CCTV CAMERA LOCATED IN VESTIBULE 101. CONFIRM EXACT LOCATION ON SITE.
- PROVIDE ONE (1) 53mm CONDUIT FROM "STOP WHEN FLASHING" PUSH BUTTON TO RADIO ANTENNA LOCATED ON ROOF OF HOSE-TOWER 130. CONFIRM EXACT LOCATION WITH SIGNALLING CONTRACTOR PRIOR TO INSTALLATION.
- PROVIDE JUNCTION BOX FOR MECHANICAL CONTROLS TO BE MOUNTED IN CEILING SPACE AS SHOWN. CONFIRM EXACT LOCATION WITH MECHANICAL CONTRACTOR PRIOR TO INSTALLATION.

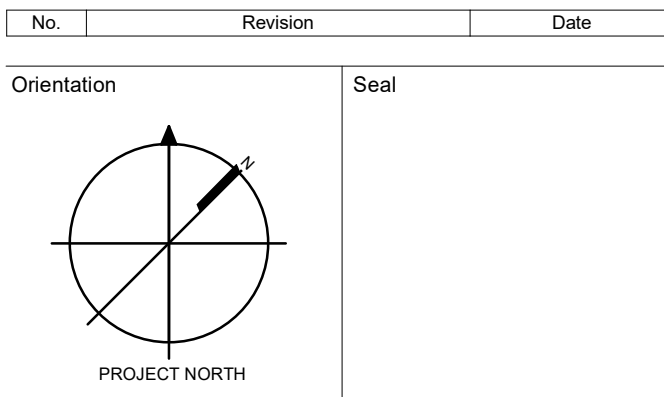


LEVEL 1 PLAN - POWER & SYSTEMS

SCALE: 1 : 100

FOR QUESTIONS REGARDING THIS PROJECT, PLEASE
EMAIL: CM-20-063@QUASARCG.COM

No.	Revision	Date
J	ADDENDUM E03	2021-10-28
I	ADDENDUM E01	2021-10-28
H	ISSUED FOR TENDER	2021-08-12
G	ISSUED FOR BUILDING PERMIT	2021-07-27
F	90% CD	2021-05-03
E	SPA	2021-03-12
D	50% CD	2021-02-05
C	BUILDING PERMIT	2021-02-05
B	PERMIT/SPA COORDINATION	2021-02-02
A	100% DESIGN DEVELOPMENT	2021-01-19



The specifications are to be considered as an integral part of these drawings and neither the drawings nor the specifications shall be used alone. Refer to architectural drawings for dimensions. Do not scale.

© Copyright Reserved:
These drawings and all that is represented herein are the exclusive property of Quasar Consulting Group.
They may not be used or reproduced without written permission from Quasar Consulting Group.



250 ROWNTREE DAIRY RD, WOODBRIDGE, ON
TEL: 905-507-0800
WEB: WWW.QUASARCG.COM

Project Information
BFES Station 201
(SPA-2021-0032)

27 Rutherford Rd. S., Brampton, ON, L6W 3J3

For
City of Brampton Fire & Emergency Services

Drawing Title
LEVEL 1 PLAN - POWER & SYSTEMS

Date	2021-10-28	Project No	CM-20-063	Drawing No	E301
Drawn by	DTH				
Scale	As indicated				

Project Name:	City of Brampton Fire Station 201	Date Issued:	October 29, 2021
Quasar Project #:	CM-21-083		
Client Project #:	20019		

Distribution

Salter Pilon Architecture	Ryan Stitt	rstitt@salterpilon.com
Salter Pilon Architecture	Brandon Bortoluzzi	bbortoluzzi@salterpilon.com
Salter Pilon Architecture	Nick Laurin	nlaurin@salterpilon.com

Addendum #: 3**Revision #:** 0

This Addendum forms part of the Contract Specifications and Drawings, and modifies the Bidding Documents, with Amendments and Additions noted below. This Addendum shall be added to the front of the specifications as issued. Bidders shall acknowledge receipt of this Addendum in the space provided in the Bid Form and include in bid amount.

This addendum includes modifications to the drawings as summarized below. Unless otherwise noted, all drawings listed below are attached herewith. Answers to Requests For Information below shall form part of the project specifications and are identified in bold following QCG (Quasar Consulting Group).

Requests for Information:

1. There are three motorized dampers shown on drawing M302 related to Compressor Room 129. A sequence of operation has not been provided for these dampers. Please clarify if these dampers are to be controlled from the BAS and if so please provide a sequence of operation. **QCG: Sequence added with this addendum.**

Changes to Drawings:

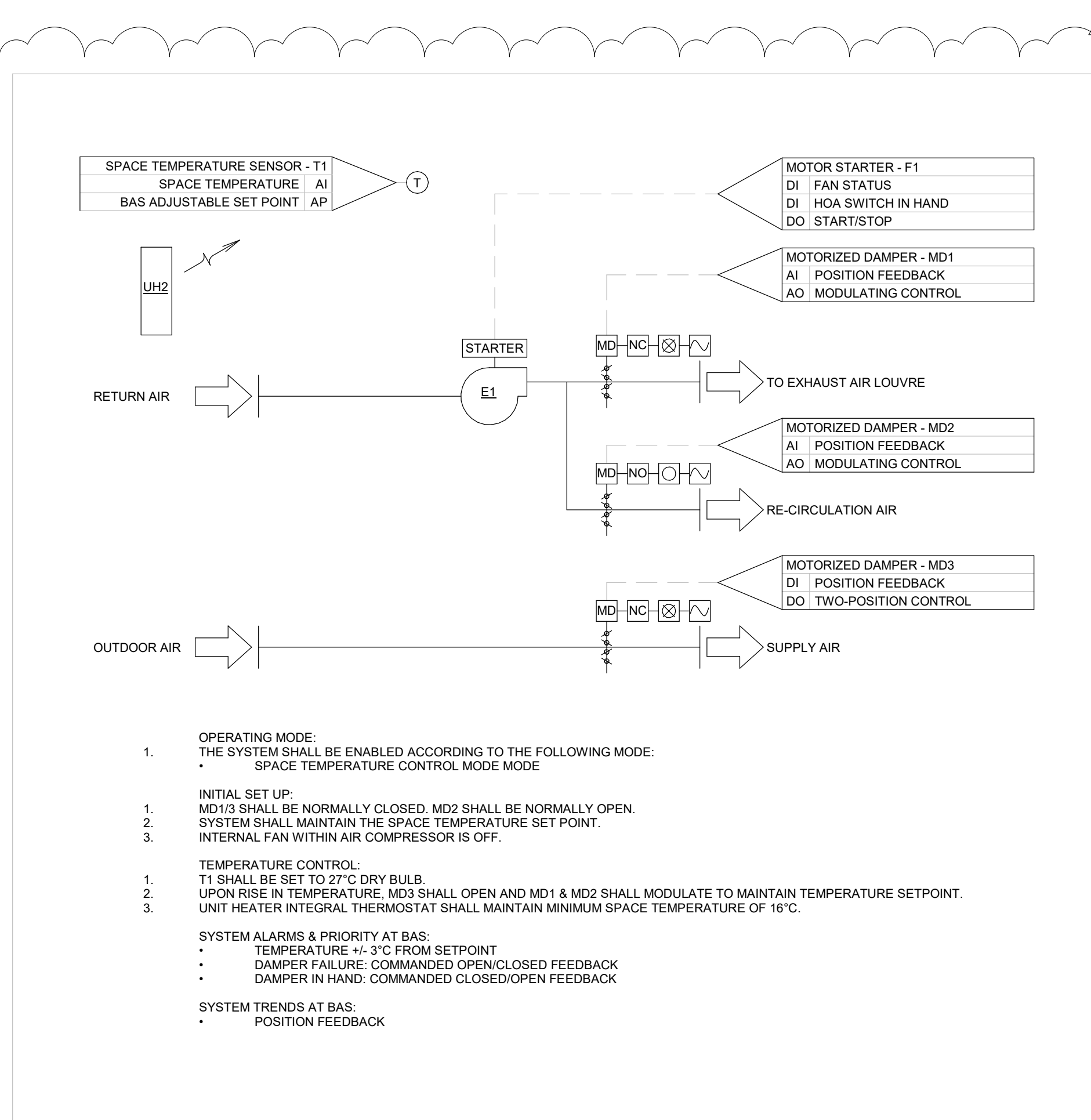
1. **Drawing M652 CONTROL SEQUENCES III**

Refer to attached drawing and note the following revision:

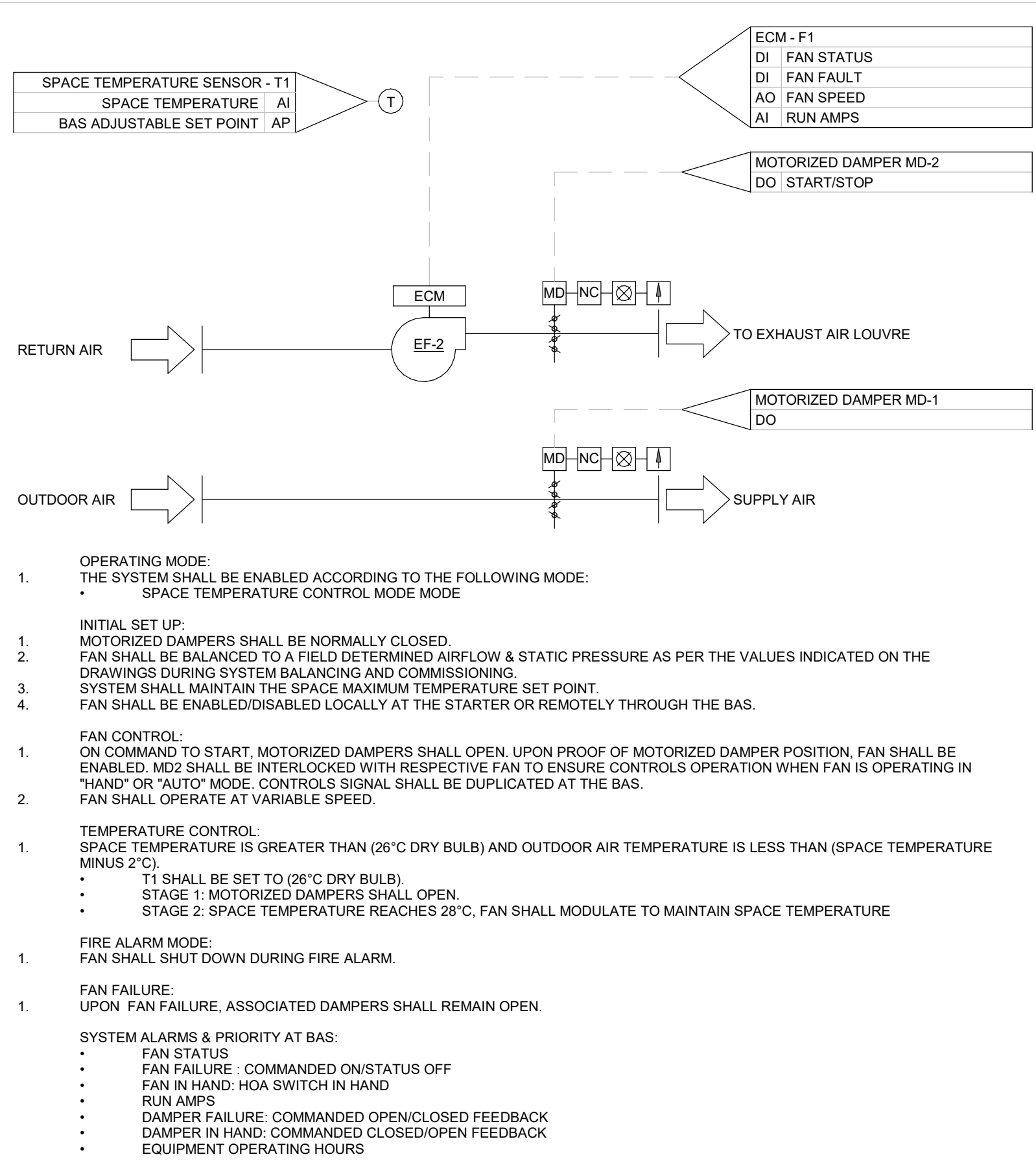
- a. Addition of SCBA Compressor Room control sequence.

Quasar Consulting Group

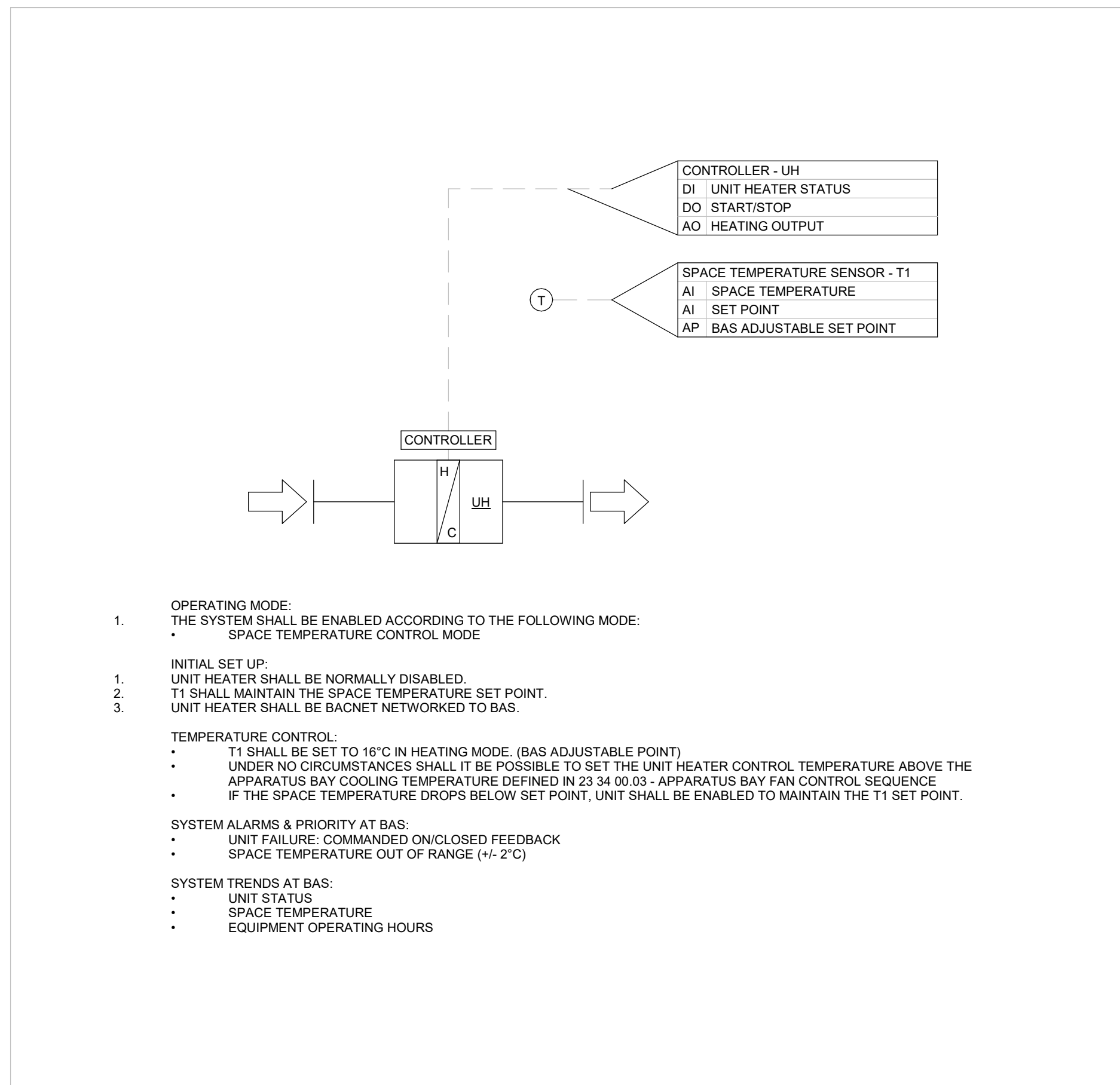
Craig Watson, P.Eng.
Team Lead - Commercial



NOT TO SCALE



NOT TO SCALE



NOT TO SCALE

FOR QUESTIONS REGARDING THIS PROJECT, PLEASE
EMAIL: CM-20-063@QUASARCG.COM

C	ADDENDUM M03	2021-10-29
B	REISSUED FOR BUILDING PERMIT	2021-09-15
A	ISSUED FOR TENDER	2021-08-12
No.	Revision	Date

Orientation	Seal
-------------	------

The specifications are to be considered as an integral part of these drawings and neither the drawings nor the specifications shall be used alone. Refer to architectural drawings for dimensions. Do not scale.

© Copyright Reserved:
These drawings and all that is represented herein are the exclusive property of Quasar Consulting Group.
They may not be used or reproduced without written permission from Quasar Consulting Group.



250 ROWNTREE DAIRY RD, WOODBRIDGE, ON
TEL: 905-507-0800
WEB: WWW.QUASARCG.COM

Project Information

BFES Station 201
(SPA-2021-0032)

27 Rutherford Rd. S., Brampton, ON, L6W 3J3

For
City of Brampton Fire & Emergency Services

Drawing Title

CONTROL SEQUENCES III

Date	2021-10-29	Project No	Drawing No		
Drawn by	Author			CM-20-063	M652
Scale	1 : 1				