



Smith + Andersen

1100–100 Sheppard Ave. East, Toronto ON M2N 6N5

416 487 8151 f 416 487 9104 smithandandersen.com

ELECTRONIC SAFETY AND SECURITY SPECIFICATION

PROJECT NAME:

NORTHERN BIRCH CREDIT UNION OFFICE FIT-UP

9-11 MADISON AVENUE

TORONTO, ONTARIO

OUR PROJECT NUMBER:

17488.003.ESS.001

DATE:

2026-01-29

ISSUED / REVISION:

PERMIT/TENDER

28.00.00.00 Index

SECTION	NAME	Page #
28.00.00.00	Index	1
28 00 05.00	Administrative Requirements	2
28 00 05.30	Codes, Standards, and Regulations	8
28 00 06.00	Fire Stopping and Water Proofing	12
28 01 00.00	General Instructions for ESS Sections	16
28 01 01.00	Operation and Maintenance of Electronic Safety and Security	26
28 05 00.00	Common Work Results for Electronic Safety and Security	28
28 05 03.00	Record Drawings	30
28 05 04.00	Submittals – Shop Drawings	33
28 05 05.20	Definitions and Abbreviations	35
28 05 13.00	Conductors and Cables for Electronic Safety and Security	41
28 05 26.00	Grounding and Bonding for Electronic Safety and Security	44
28 05 28.00	Pathways for Electronic Safety and Security	46
28 05 53.00	Identification for Electronic Safety and Security	49
28 08 00.00	Commissioning of Electronic Safety and Security	51
28 08 00.00	Access Control	55
28 16 00.00	Intrusion Detection	80
28 23 00.00	Video Surveillance	92
28 26 00.00	Electronic Personal Protection System	103
28 40 00.00	Electronic Safety and Security Systems Integration	108
28 51 00.00	Intercom System	120

END OF SECTION

28 00 05.00 Administrative Requirements

1. General

1.1. PROJECT CLOSEOUT SUBMITTALS

1.1.1. Provide the following project closeout submittals:

- .1 Table of content
- .2 As-built drawings
- .3 Commissioning test results and reports for each device, each system, and each function
- .4 Commissioning results for each video surveillance camera complete with sample field of view image
- .5 Systems settings, configuration, and documentation
- .6 Operation and Maintenance Manuals
- .7 Warranty Letters and Certificates
- .8 Cyber Security Report Letter

1.1.2. Mark all changes and deviations on construction drawing(s) during the construction process, including all conduit and cable pathways to and from equipment.

1.1.3. Update Asbuilt drawing(s) during construction.

1.1.4. Include all additional devices and cables installed during the project on Asbuilt drawings. The Electronic Safety and Security Engineer's Representative will review the status of the as-built drawing(s) from time to time during the construction process. On completion of the project, forward to the Electronic Safety and Security Engineer's Representative electronic drawings indicating all such changes and deviations for review within 10 business days of the completion of the project.

1.1.5. Request (via email) from the Electronic Safety and Security Engineer's Representative a soft copy of drawings for use in preparation for Record Drawings.

1.1.6. Return record drawing(s) via secure file transfer using the latest native drawing file format or better. If this requirement cannot be met, Smith + Andersen will update all hand-drawn Record Drawings to the native drawing file format. The cost for this service is based on Smith + Andersen's per diem rates at the time of completion. Pay for all costs associated with this work.

1.1.7. The project is incomplete and a holdback will be retained until satisfactory as-built drawing(s) are provided.

1.2. SUBMITTALS – TESTING, AND COMMISSIONING

1.2.1. Provide testing and commissioning documentation in soft format for all items and their related components to the Electronic Safety and Security Engineer's Representative before the completion of the project or at the Electronic Safety and Security Engineer's Representative's request. Include maintenance manuals and operating instructions for the Owner's staff use.

- 1.3. PERMITS, LICENSE REVIEWS, AND FEES
 - 1.3.1. Where materials are specified which require special approval of CSA or local authorities obtain such approval for the particular installation with the cooperation of the material supplier.
 - 1.3.2. Submit required documents and shop drawings to authorities having jurisdiction to obtain approval for the work. Prepare any additional information, details, and drawings that these authorities may require.
- 1.4. ALTERNATE PRODUCT
 - 1.4.1. This document specifies the use of devices manufactured, warranted, and certified by respective manufacturers. Alternate materials is not be accepted unless specifically noted.
 - 1.4.2. Where the provision of the materials would compromise the schedule, submit a request to use an alternate product to the Electronic Safety and Security Engineer's Representative. Depending on the circumstance, the Electronic Safety and Security Engineer's Representative may provide written authorization to substitute the Product. The written authorization is to be obtained before alternatives are purchased or installed.
- 1.5. SEISMIC FORCE RESTRAINT SYSTEM.
 - 1.5.1. Provide all seismic resisting systems for all Electronic Safety and Security systems equipment.
 - 1.5.2. Definitions
 - .1 Low: Buildings that represent a Low Direct or Indirect Hazard to human life in the event of failure.
 - .2 Normal: All buildings except those listed in the Importance Categories Low, High and Post-disaster.
 - .3 High: Buildings likely to be used as Post-disaster shelters and manufacturing or storage facilities containing toxic, explosive or other hazardous substances in sufficient quantities to be dangerous to the public if released.
 - .4 Post-disaster: Buildings that are required to be operational after a disaster.
 - .5 SFRS: Acronym for Seismic Force Restraint System.
 - .6 SCS: Acronym for Slack Cable Restraint System.
 - .7 Seismic Consultant: A Professional Structural Engineer licensed in the respective jurisdiction who specializes in the seismic restraint of building elements and the design of SFRS.
 - 1.5.3. Fully integrate SFRS into, and make compatible with:
 - .1 Noise and vibration controls specified elsewhere in this project specification, and
 - .2 Systems, and equipment not required to be operational during and after seismic event.
 - 1.5.4. Provide SFRS that during a seismic event prevent systems and equipment from causing personal injury and from moving from normal position.
 - 1.5.5. Obtain the services of a Professional Engineer, licensed in the Province / Territory of the Place of the Work, and specializing in the design of SFRS, to provide the necessary design and details for a complete SFRS including systems of structural supports and brazing of all relevant equipment as required to comply the applicable Building Codes. Require this Professional Engineer be responsible for ensuring that the installation conforms to the design.
 - 1.5.6. Submit Shop Drawings and product data for review by the Electronic Safety and Security Engineer Representative.

- 1.5.7. Shop Drawing Submittals to include:
- .1 Full details of design criteria,
 - .2 Working drawings, materials lists, schematics full specifications for all components of each SFRS to be provided,
 - .3 Design calculations including restraint loads resulting from seismic forces in accordance with all applicable Codes,
 - .4 Separate Shop Drawings for each SFRS and devices for each system, equipment,
 - .5 Identification of location of each device,
 - .6 Schedules of types of SFRS equipment and devices,
 - .7 Details of fasteners and attachments to structure, anchorage loadings, attachment methods,
 - .8 Installation procedures and instructions, and
 - .9 These drawings are designed and bear the signed stamp of a Professional Engineer licensed to practice in the appropriate discipline and in the Place of Work.
- 1.5.8. Provide positive seismic and wind resisting on those systems and components required by the Building Code and the Authority Having Jurisdiction.
- 1.5.9. Coordinate all SFRS with all the Architect and all affected trades.
- 1.5.10. Provide SFRS for conduit systems that is compatible with:
- .1 Expansion, anchoring, and guiding requirements.
 - .2 Equipment vibration isolation and equipment SFRS.
- 1.5.11. Do not utilize cast iron, threaded pipe, and other brittle materials as part of SFRS.
- 1.5.12. Ensure seismic control measures do not interfere with integrity of fire stopping.
- 1.5.13. Equipment installed on vibration isolation that requires seismic restraint must comply with the noise and vibration controls specified elsewhere in this project specification.
- 1.5.14. Install SFRS at least 25 mm from all other equipment, systems, and/or services.
- 1.5.15. Co-ordinate connections with all disciplines.
- 1.5.16. Install SFRS in accordance with the Seismic Professional Engineer's design.
- 1.5.17. Following the completion of the installation of the seismic resisting systems, have the designing engineer submit a stamped letter stating that the installation has been completed in accordance with the applicable Building Codes and their design. Require the engineer to complete and submit signed and sealed letters of assurance (e.g. Schedules, where applicable) and letters of compliance for all equipment that requires seismic resisting in accordance with latest codes, standards and requirements of the Authorities Having Jurisdiction.
- 1.5.18. Require engineer to include additional documentation to identify the equipment and device types and quantities that were reviewed to ensure that all components requiring seismic resisting were completed.
- 1.5.19. Require engineer to indicate in letters that "All Electronic Safety and Security equipment shown on the Smith and Andersen Drawings has been seismically resisted in accordance with the local Building Code."

1.6. SCHEDULING

- 1.6.1. Within one week of the award of the contract submit a formal project schedule to the Electronic Safety and Security Engineer's Representative showing the start and finish dates of major tasks as denoted by System, material order, and delivery to site, installation, testing, and commissioning.
- 1.6.2. Submitted updated schedules as requested by the Electronic Safety and Security Engineer's Representative.

1.7. PROJECT MANAGEMENT

- 1.7.1. Provide complete project management for this project. Complete project management include:
- .1 Develop a detailed Gantt chart project plan and submit it to the Owner and Electronic Safety and Security Engineer's Representative for review and approval before the start of the project.
 - .2 Chair biweekly construction meetings for the duration of the project. Construction meetings will be on-site or via conference call at the Owner's and or Electronic Safety and Security Engineer's Representative's discretion.
 - .3 Generate and submit detailed biweekly construction progress reports to the Owner and Electronic Safety and Security Engineer's Representative. Include in each progress report itemized detailed description and extent of tasks completed, itemized detailed description and quantification of materials installed, and labeled photos that clearly show the extent of construction progress.

1.8. PROJECT MEETINGS

- 1.8.1. Attend site meetings when requested by the Electronic Safety and Security Engineer's Representative and/or the Project Manager. Regular meetings may occur once per week at the Electronic Safety and Security Engineer's Representative's and/or the Project Manager's discretion.
- 1.8.2. Attend weekly project meetings throughout the project to review the status of current and planned activities, schedule, and conduct other business associated with the project.

1.9. PROGRESS REPORTS

- 1.9.1. Issue a status report at the weekly project meeting including the status of progress, project completion for phases, material ordering, and delays.

1.10. CLEANUP

- 1.10.1. Keep the site and surrounding area clean, safe, and free from debris at all times. Remove all debris from the site daily.
- 1.10.2. Upon completion of the work and before acceptance and final payment is made, remove from the site, all surplus and discarded materials, temporary structures, and debris of every kind. Dispose of surplus and waste materials removed from the site following applicable laws and regulations.

1.11. ACCEPTANCE

- 1.11.1. Before acceptance by the Electronic Safety and Security Engineer's Representative, all the equipment and cabling must be installed, cleaned, tested commissioned. At points of termination, all cabling and terminations must be labeled and must be free of any cable pulling lubricants before acceptance by the Electronic Safety and Security Engineer's Representative.

1.12. REVIEW AND TESTING REQUIREMENTS

- 1.12.1. Develop a testing and commissioning checklist for each system and submit it to the Electronic Safety and Security Engineer's Representative for approval 10 business days before commissioning commences.
- 1.12.2. The Electronic Safety and Security Engineer's Representative must approve the testing and commissioning procedure before the commencement of testing and commissioning and may request to be present.
- 1.12.3. Invite the Electronic Safety and Security Engineer's Representative to witness field testing and commissioning and notify them of the start date of the testing phase 10 business days before testing and commissioning commence.
- 1.12.4. Test and commission all electronic safety and security systems.

1.13. BIDDER INQUIRIES

- 1.13.1. Not Used.

1.14. BID FORM AND SUBMISSION OF BIDS

- 1.14.1. Not Used.

1.15. PROGRESS DRAWS

- 1.15.1. Not Used.

1.16. QUOTES FOR CONTEMPLATED CHANGE NOTICES

- 1.16.1. Itemize all quotes for contemplated changes notices and include the following:
- .1 Itemised list of each device including respective make, model, and quantity quoted and unit price
 - .2 Total labour hours for installing and configuring each device
 - .3 Total length of wiring quoted for each device and labour hours for installing the quoted wiring
 - .4 Total length of conduit quoted for each device wiring and labour hours for installing the quoted conduit.
 - .5 Labour rate
 - .6 Subtotal cost of all materials/devices
 - .7 Subtotal cost of all labour
 - .8 Total quote value

1.17. HOLDBACK

- 1.17.1. Not Used.

1.18. SCHEDULE

1.18.1. Not Used.

1.19. LABOUR

1.19.1. Comply with all project job-site requirements for the duration of the project.

1.19.2. Do not assign or sub-contract any work without the prior written consent of the Project Manager. With the Tender Response submit a list of subcontractors.

1.19.3. For all work related to this project, use only tradesmen who are fully trained, qualified, and experienced in the installation and commissioning of the Electronic Safety and Security Systems.

2. Products

2.1. NOT USED

3. Execution

3.1. NOT USED

END OF SECTION

28 00 05.30 Codes, Standards, and Regulations

1. General

1.1. CODES, STANDARDS, AND REGULATIONS COMPLIANCES

- 1.1.1. Adhere to the latest edition of all applicable Codes, Standards, Regulations, and documents listed throughout this document.
- 1.1.2. All products installed must meet or exceed all Local, Provincial, and Federal Building, Fire, Health, Safety, and Electrical Codes.
- 1.1.3. Ensure that Non-plenum and plenum-rated cables are ETL or ULC (UL) Listed and CSA Certified as type CMR / CMP (respectively).
- 1.1.4. The equipment, material, and installation conform to the latest version of the applicable Codes, Standards, and Regulations of authorities having jurisdiction as indicated in the table below. In the case of conflict or discrepancy the more stringent code, standard or regulation will apply.

STANDARD	TITLE
ANSI/ICEA	
S-80-576	Standard for Category 1 & 2 Individually Unshielded Twisted Pair Indoor Cables (With or Without an Overall Shield) for Use in Communications Wiring Systems Technical Requirements
S-83-596	Optical Fibre Premises Distribution Cable, latest version
S-87-640	Optical Fibre Outside Plant Communications Cable, latest version
S-104-696	Standard for Indoor-Outdoor Optical Cable, latest version
Z136.2	American Standards for the Safe Operation of Optical Fibre Communication Systems Utilizing Laser Diode and LED Sources
TIA/EIA	
455-C	Optical Fibre Test Procedures
568-1-D	Commercial Building Telecommunications Cabling Standard: General Requirements
568-C.2	Commercial Building Telecommunications Cabling Standard: Balanced Twisted Pair Cabling
568-C.3-D	Commercial Building Telecommunications Cabling Standard: Optical Fibre Cabling Components Standard
569-D	Commercial Building Standard for Telecommunications Pathways and Spaces including all addenda
606-C	Administration Standard for Telecommunications Infrastructure
607-C	Telecommunications Grounding (Earthing) and Bonding for Customer Premises
758-B	Customer Owned Outside Plant Telecommunications Cabling Standard.
862-B	Structured cabling infrastructure Standard for Intelligent Building Systems

RS232C	Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
RS485	Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems
CSA	
C22.1-18	Canadian Electric Code Part I: Safety Standards for Electrical Installations.
C22.2 No. 182.4-M90	Plugs, Receptacles, and Connectors for Communication Systems. R2015
C22.2 No. 214-17	Communications Cables
CAN/CSA-C22.2 No. 0-10	General Requirements, Canadian Electrical Code, Part II (latest version)
CAN/CSA-C22.2 232-17	Canadian Electric Code Part II: Optical Fibre Cables.
C22.2 NO. 205-12	Signal Equipment
T527-94	Grounding and Bonding for Telecommunications in Commercial Buildings
T528-93	Design Guidelines for Administration of Telecommunications Infrastructure in Commercial Buildings.
T529-95	Design Guidelines for Telecommunications Wiring Systems in Commercial Buildings.
T530-99	Building Facilities, Design Guidelines for Telecommunications
NFPA	
NFPA70	National Electrical Code
OTHER	
CAN/ULC-S115:2018	Standard Method of Fire Tests of Firestop Systems
CAN/ULC-S101-14	Standard Method of Fire Endurance Tests of Building Construction and Materials
CAN/ULC-S102 latest version	Standard Method of Testing for Surface Burning Characteristics of Building Materials and Assemblies
CAN/ULC S316-14	Standards for Performance of Video Surveillance Systems
CAN/ULC S319-05	Electronic Access Control Systems
CLC	Canada Labour Code, Part II Occupational Health and Safety, and Provincial and Local Health and Safety regulations
UL 294	The Standard of Safety for Access Control System Units
UL 365	Police Station Connected Burglar Alarm Units and Systems
ULC1076	Proprietary Burglar Alarm Units and Systems
UL 609	The Standard of Safety for Local Burglar Alarm Units and Systems
UL 639	Standard for Intrusion-Detection Units
UL 1610	Standard for Central-Station Burglar-Alarm Units
ULC-S306-03	The Standard of Safety for Intrusion Detection Units
UL 969	Standard for Marking and Labeling Systems
UL 1037	Standard for Antitheft Alarms and Devices
UL 1067	Standard for Electrically Conductive Equipment and Materials for Use in Flammable Anesthetizing Locations
UL 1492	Standard for Audio-Video Products and Accessories

UL 2044	Standard for Commercial Closed-Circuit Television Equipment
CEC, Part 1	The Canadian Electrical Code, Part 1
CSA ISO/IEC 11801	Information Technology: Generic Cabling for Customer Premises
ICEA S-80-576	Individually Unshielded Twisted Pair Indoor Cable for Use in Communications Wiring Systems
IEEE Std 1100	IEEE Specified Practice for Powering and Grounding Electronic Equipment (IEEE Emerald Book)
IEC 603-7, Part 7	Detailed Specifications for Connectors, 8-Way, Including Fixed and Free Connectors with Common Mating Schemes
ISO/IEC IS 11801A	Generic Cabling for Customer Premises
WC 63.1	Performance Standard for Field Testing of Unshielded Twisted-Pair Cabling System
OHSA	Occupational Health and Safety Act - R.S.O. 1990, c. 0-1
UL 444 and 13	Adopted Test and Follow-Up Service Requirements For The Optional Qualification of 100Ω Twisted-Pair.
CCTA	Canadian Cable Television Association
NCTA-02/89 rev. 93	NCTA Specified Practices for Measurements on Cable Television Systems.
Industry Canada	ICES 003 Emissions
RoHs	Restriction of Hazardous Substances Directive 2011/65/EU
Subpart B	RF Emissions
CE Standards	EN 55022 RF Emissions
CE Standards	EN 55024 RF Immunity
FCC	Federal Communications Commission
FCC Part 15	Radio Frequency Device
FCC Part 68	Connection of Terminal Equipment to the Telephone Network
CE Standards	EN 60950-1 Equipment Safety
OESC	Ontario Electrical Safety Code – latest edition.
O.R. 388/97	Ontario Fire Code – latest edition.
O.R. 403/97	Ontario Building Code – latest edition.

- 1.1.5. Comply with applicable Electrical Safety Code, all Local, Provincial and Federal laws, where applicable, and with requirements of the Canadian Standards Association (CSA) when mandatory. Make any changes or alterations required by the authorized inspector of the authority having jurisdiction, at no extra charge to the Owner.

2. Products

2.1. NOT USED

3. Execution

3.1. CODE, STANDARD, AND REGULATION COMPLIANCES

3.1.1. All cables and components installed and terminated following CSA. Particular attention is given to ensuring proper distance is kept from fluorescent light fixtures, electrical cables, or any other source of EMI. Cables are combed and bundled in a neat and organized manner. The Electronic Safety and Security Engineer's Representative determine the neatness of the installation. At no extra-cost, Cables are redressed that have not been properly combed and dressed. Coordinate with the Electronic Safety and Security Engineer's Representative before termination in any Telecom Rooms.

3.1.2. The equipment manufacturer's specifications must not be exceeded by the horizontal run length. If the constraint cannot be met, notify the Electronic Safety and Security Engineer's Representative of any cables that exceed the equipment manufacturer's stated limitations. Include for rectification of the limitation in their bid. Rectifications include active and passive devices, signal boosters, signal extenders, protocol converts, installation of wire gauge suitable to the cabling length being installed, and/or a combination of the aforementioned.

END OF SECTION

28 00 06.00 Fire Stopping and Water Proofing

1. General

1.1. WORK INCLUDED

1.1.1. Fire Stopping

- .1 Provide seals in all Fire Rated Separations and Firewalls to form tight barriers to retard the passage of flame and smoke.
- .2 The installed seals provide and maintain the fire-resistance rating of the adjacent floor, wall, or other fire separation assembly to the Code Requirements.
- .3 Provide moisture seals as well as fire and smoke seals for all floor penetrations.
- .4 Provide Fire Stop pillows for existing cable tray penetrations through firewalls.
- .5 Re-establish the integrity of all fire-rated structures and assemblies that they have created or disturbed.
- .6 For this specification, only Fire Stop Systems that have been tested to the applicable ULC Standard are acceptable.
- .7 Provide non-permanent CSA approved Fire Stop systems that are dielectric, water-resistant, non-hardening, permanently pliable/re-enterable putty along with the appropriate damming or backer materials (where required).
- .8 All fire stopping maintain a minimum one-hour rating and meet applicable Federal, Provincial and Local building codes.
- .9 Following the Standards, all Fire Stop Systems are listed and tested by an SCC and accredited Third-Party Testing Agency.
- .10 Fire-resistance rating of the surrounding Fire Separation or Firewall is less than the Fire resistance ratings of installed Fire Stop Systems.
- .11 All Smoke Seals selected for use should comply with Standards.
- .12 To allow for building settling and seismic movement, ensure all Fire Stop Materials and Smoke Seals have elastomeric characteristics. Verify all Fire Stop Materials and Smoke Seals are free of asbestos.

1.1.2. Water Proofing

- .1 Seal all foundation penetrating conduits and service entrance conduits and sleeves to eliminate the intrusion of moisture and gases into the building. This requirement also includes spare conduits.
- .2 Upon cable placement all service entrance conduits through the building are sealed or resealed. Spare conduits are plugged with expandable plugs.

1.1.3. Quality Assurance

- .1 Provide fire stopping systems that comply with the following requirements following:
 - .1 Fire stopping tests are performed by a qualified, testing and inspection agency. A qualified testing and inspection agency is UL, or another agency performing testing and follow-up inspection services for fire stop system acceptable to authorities having jurisdiction.
 - .2 Fire stopping products bear the classification marking of qualified testing and inspection agency

- .2 Provide the work of this Section using competent installers, experienced in the application of the materials and systems being used, approved, and trained by the material or system manufacturer.
 - .3 Fire Stop Systems conform to the fire (F), hose (H), and temperature (T) ratings of Codes.
 - .4 Fire Stop Materials and Smoke Seal materials must have a flame spread rating of 25 or less, National Fire Protection Association (NFPA Class "A").
 - .5 For this specification, the only acceptable Fire Stop Systems are those that have been tested to the CAN/ULC S115 Standard.
- 1.1.4. Performance
- .1 Fire-rated pathway devices are the preferred product and install these devices in all locations where frequent cable moves, add-ons, and changes are anticipated.
 - .2 Where non-mechanical products are utilized, provide products that upon curing do not re-emulsify, dissolve, leach, break down, or otherwise deteriorate over time from exposure to atmospheric moisture, sweating pipes, ponding water, or other forms of moisture characteristic during or after construction.
 - .3 Where it is not practical to use a mechanical device, openings within floors and walls designed to accommodate telecommunications and data cabling are provided with re-enterable products that do not cure or dry.
 - .4 Openings for cable trays are sealed using re-enterable fire-stopping pillows.
- 1.1.5. Project Conditions
- .1 Do not install fire stopping products when ambient or substrate temperatures are outside limitations specified by the manufacturer
 - .2 Do not install fire-stopping products when substrates are wet due to rain, frost, condensation, or other causes.
 - .3 Maintain minimum temperature before, during, and for a minimum of 3 days after installation of materials.
 - .4 Do not use materials that contain flammable solvents.
 - .5 Coordinate construction of openings and penetrating items to ensure that through-penetration fire stop systems are installed according to specified requirements.
 - .6 Coordinate sizing of sleeves, openings, core-drilled holes, or cut openings to accommodate through-penetration fire stop systems.
 - .7 Schedule installation of fire stopping after completion of penetrating item installation but before covering or concealing of openings.
2. Products
- 2.1. GENERAL
- 2.1.1. Use only fire-stopping products that have been tested for specific fire-resistance-rated construction conditions conforming to construction assembly type, penetrating item type, annular space requirements, and fire rating involved for each separate instance.
- 2.2. APPROVED MANUFACTURERS
- 2.2.1. Products manufactured by Hilti (or approved equivalent) are acceptable.

2.2.2. Obtain fire stop systems for each type of penetration and construction condition indicated only from a single manufacturer.

2.3. MATERIALS

2.3.1. Firestop Sealants: The following products are acceptable.

- .1 Hilti FS-ONE high-performance Intumescent Firestop Sealant
- .2 Hilti CP 601S Elastomeric Firestop Sealant.
- .3 Hilti CP 606 Flexible Firestop Sealant
- .4 Hilti CP 604 Self-Leveling Firestop Sealant

2.3.2. Cast-In Firestop Device: A one-step cast-in firestop device for a variety of pipe materials and diameters. The following product is acceptable.

- .1 Hilti CP 680-M Cast-in Firestop Device

2.3.3. Firestop Putty: An intumescent, non-hardening, firestop putty for cable and pipe penetrations. The following product is acceptable:

- .1 Hilti CP 681 Firestop Putty Stick.

2.3.4. Firestop Plug: Ready-to-use intumescent and reusable plug for small openings. The following product is acceptable:

- .1 Hilti CP 658T Firestop Plug.

2.3.5. Fire Rated Cable Pathways: Re-penetrable cable management device:

- .1 Hilti CP 653 Speed Sleeve.

3. Execution

3.1. FIRE STOPPING

3.1.1. Before beginning installation, verify that substrate conditions previously installed under other sections are acceptable for the installation of fire stopping following the manufacturer's installation instructions and technical information

3.1.2. Examine sizes and conditions of Fire Stop Material voids. Fill and or correct Fire Stop Materials to eliminate voids.

3.1.3. Ensure Surfaces are free of dirt, grease, oil, scale, laitance, rust, release agents, water repellents, and any other substances that may inhibit optimum adhesion

3.1.4. Prepare surfaces in contact with Fire Stop Systems and Smoke Seals to the manufacturer's instructions. Mask where necessary to avoid spillage and overcoating onto adjoining surfaces; remove stains on adjacent surfaces.

3.1.5. Install/replace sound barrier/fire stopping materials as soon as cables have been pulled through the opening.

3.1.6. Before, during, and after installation of sealant Fire Stop Materials make sure all Fire Stop Systems that require mineral wool or ceramic fibre backer or filler materials, these materials are dry and free of other contaminants. Alkaline water contamination of the backer or filler materials may cause corrosion of metallic penetrating items.

- 3.1.7. Apply Fire Stop Systems and Smoke Seals in strict accordance with manufacturer's instructions to prevent the passage of fire and smoke, and where required or specifically designated, the passage of fluids
- 3.1.8. Provide temporary forming and packing as required. Tool or trowel all exposed surfaces to a smooth, tidy finish.
- 3.1.9. Fire Stop and smoke seal gaps and holes in all Fire Separation and Firewall construction through which cables pass as a result of work in this document.
- 3.1.10. In Combustible Construction (membrane GWB type) where the framing members are wood or where paper-faced insulation is incorporated within the separation, a Fire and Temperature rise "FT" rating is required equal to that of the rating of the Fire Separation. Include openings that have been formed and sleeved.

- 3.2. WATERPROOFING
 - 3.2.1. Conduits with cables in them are permanently sealed by firmly packing the void around the cable with oakum and capping with hydraulic cement or waterproof duct seal.

- 3.3. EXPOSED SERVICE PENETRATIONS IN CEILING OF UNDERGROUND PARKING AREAS
 - 3.3.1. Where the bottom of a Fire Stop System is exposed, seal the bottom side of the assembly with a fire-rated elastomeric Fire Stop sealant.

- 3.4. CLEAN UP
 - 3.4.1. Remove excess materials and debris and clean adjacent surfaces immediately after application to satisfaction of the Project Manager. Remove and or correct staining and discoloring of adjacent surfaces as directed.

END OF SECTION

28 01 00.00 General Instructions for ESS Sections

1. General
 - 1.1. WORK INCLUDED
 - 1.1.1. Conform to the requirements of Divisions 0 and 1, which apply to and form part of all sections of the work.
 - 1.1.2. The more stringent and/or more onerous requirement is applied if there is a conflict between the requirements outlined in this Electronic Safety and Security specifications document and requirements indicated in Divisions 0 and 1.
 - 1.1.3. Read and comply with all sections of this document.
 - 1.1.4. The Specification is divided into Sections that are not intended to identify contractual limits between sub-contractors nor between the contractor and sub-contractors. The requirements of anyone Section apply to all Sections. Refer to other Divisions and Sections to ensure a complete and operational system.
 - 1.1.5. Provide Electronic Safety and Security components and accessories which may not be specifically shown on the Drawings or stipulated in the Specifications, but are required to ensure complete and operational systems.
 - 1.1.6. Provide all labour, materials, tools, and equipment required for the complete installation, commissioning and start-up of Electronic Safety and Security systems called for in all sections of the Contract Documents.
 - 1.2. SECTIONS AFFECTED
 - 1.2.1. These instructions apply to and form a part of all Electronic Safety and Security Sections.
 - 1.3. SCOPE OF WORK
 - 1.3.1. Include all necessary wiring, cabling, labor, tools, equipment, and ancillary materials required to furnish and install complete and operational Electronic Safety and Security Systems.
 - 1.3.2. This specification includes a general description as well detailed functional and technical requirements for the Electronic Safety and Security Systems.
 - 1.3.3. This specification provides all information necessary to produce a complete proposal for scalable multi-user, multi-tasking Electronic Safety, and Security Systems. The Electronic Safety and Security Systems include all computer hardware and software, controllers, interfaces, card readers/keypads, credentials, video recorders, cameras, alarm sensing devices, communication devices, electric door locking hardware, power supplies, cable/wire, conduit, raceways, enclosures, mounting hardware, and all other equipment as indicated on contract drawings and as specified herein. Except where noted to reuse existing, ensure all materials are new, commercial-grade, and of good quality.
 - 1.3.4. Provide all work and materials mentioned in this specifications document and on associated drawings unless otherwise noted.
 - 1.3.5. This document is the Specification for the supply and installation of Electronic Safety and Security Systems for the following project:
 - 1.3.6. This project consists of the complete supply, installation, and commissioning of the following Electronic Safety and Security systems:

- .1 Access Control
 - .2 Intrusion Detection System
 - .3 Video Surveillance System
 - .4 Intercom System
 - .5 Electronic Personal Protection System
- 1.3.7. All Electronic Safety and Security systems supplied and installed are ensured that it is turnkey complete and fully operational. All Electronic Safety and Security systems is integrated as per the contract drawings and specifications.
- 1.3.8. The Electronic Safety and Security Systems is installed based on the drawing documents provided herewith.
- 1.3.9. All cables for the Electronic Safety and Security Systems is installed via conduits and or cable tray.
- 1.3.10. The scope of work includes but not limited to:
- .1 Provide of all active and passive hardware and cables as specified within this document to support the Electronic Safety and Security Systems.
 - .2 Where active and passive hardware and cabling are not specified but are required to make the Electronic Safety and Security Systems turnkey and to meet the intent, provide such active and passive hardware and cabling at no extra cost.
 - .3 Supply and installation of equipment cabinets, complete with all accessories.
 - .4 Supply and installation of backboards.
 - .5 Supply and installation of all fire stop materials/mechanisms for all penetrations.
- 1.3.11. While every attempt has been made to ensure that all information is correct at the time of publication, the products specified are available, and that the part numbers identified are correct, verify all part numbers and report any errors and omissions in this Specification prior to bid submissions.
- 1.3.12. Read this document in conjunction with the project related security drawings.
- 1.3.13. Read this document in conjunction with the project-related Door Schedule and Door Hardware Schedule.
- 1.3.14. Dimensions shown on Contract Drawings are approximate. Verify dimensions by reference to shop drawings and field measurements.
- 1.3.15. Quantities or lengths indicated in any of the Contract Documents are approximate only and not held to gauge or limit the work.
- 1.3.16. Include in bid all labour, materials, plant, transportation, storage costs, training, equipment, insurance, temporary protection, permits, reviews, bonding, taxes, and all necessary and related items required to provide a complete and operational Electronic Safety and Security Systems.
- 1.4. SCOPE MATRIX
- 1.4.1. Devices shown on drawings shows the general locations. Determine and coordinate the final locations of each devices on site with the EC to ensure that all conduits and associate backboxes are located where respective devices will be installed. Be responsible for all costs resulting from failure to execute the above.
- 1.4.2. General Requirements This responsibility matrix to be read in conjunction with the Electronic Safety and Security Specifications.

1.4.3. This responsibility matrix not be used as the sole source of scope requirements and scope delineation. Refer to the Electronic Safety and Security Specifications and associated drawings for additional information and requirements.

1.4.4. Refer to the below scope matrix for scope or responsibilities:

Legend:
DHC: Door Hardware Contractor (DIV 08)
EC: Electrical Contractor (DIV 26)
SC: Security Contractor (DIV 28)
CC: Communications Contractor (DIV 27)
AVC: Audiovisual Contractor (Div 27)

Component	Supply	Install	Commission	Requirements
Access Control				
Wired Security Doors				
Card/Credential Reader	SC	SC	SC	
Credentials	SC	SC	SC	
Door Contact	SC	SC	SC	
Electrified Lock: *Electric Strike *Electric Latch Retraction *Electric Mortise Lock	DHC	DHC	SC	Coordinate the exact mount location of devices with EC to ensure that all conduits and back boxes are installed in the optimal locations.
Maglock	DHC	DHC	SC	Security Contractor to acquire maglock Permit
Motion Request To Exit	SC	SC	SC	
Push Button Request To Exit	SC	SC	SC	
Controller	SC	SC	SC	
Controller Enclosure	SC	SC	SC	
Power Supply	SC	SC	SC	
Conduit	EC	EC	EC	Coordinate the exact mount location of devices with EC to ensure that all conduits and back boxes are installed in the optimal locations.
Category 6/IP Wiring	CC	CC	CC	
Non-Category 6/IP Wiring	SC	SC	SC	
Patch panel, patch cords	CC	CC	CC	
Server complete with: -software, -device licenses, -Integration licenses, -Client computer licenses	SC	SC	SC	
Client Computer with Software	SC	SC	SC	
Electrical circuits, power connections and receptacles	EC	EC	EC	
Intrusion Detection System				
Door Contact	SC	SC	SC	
Motion Request To Exit	SC	SC	SC	

Motion Detector	SC	SC	SC	
Keypads	SC	SC	SC	
Break Glass Detector	SC	SC	SC	
Peripheral Devices	SC	SC	SC	
Conduit	EC	EC	EC	Coordinate the exact mount location of devices with EC to ensure that all conduits and back boxes are installed in the optimal locations.
Category 6/IP Wiring	CC	CC	CC	
Non-Category 6/IP Wiring	SC	SC	SC	
Patch panel, patch cords	CC	CC	CC	
Controller	SC	SC	SC	
Controller Enclosure	SC	SC	SC	
Communicators	SC	SC	SC	
Power Supply	SC	SC	SC	
Electronic Personal Protection System				
Duress Alarm Station	SC	SC	SC	
Master Intercom Station	SC	SC	SC	
Relay	SC	SC	SC	
Power Supply	SC	SC	SC	
Conduit	EC	EC	EC	Coordinate the exact mount location of devices with EC to ensure that all conduits and back boxes are installed in the optimal locations.
Category 6/IP Wiring	CC	CC	CC	
Non-Category 6/IP Wiring	SC	SC	SC	
Patch panel, patch cords	CC	CC	CC	
Power Over Ethernet POE Extenders	CC	CC	CC	
Fibre optic cable, connectors, patch panel and patch cords	CC	CC	CC	
System Server complete with: -software, -device licenses, -Integration licenses, -Client computer licenses	SC	SC	SC	
Client Computer with Software	SC	SC	SC	
Electrical circuits, power connections and receptacles	EC	EC	EC	
Intercom /Entryphone System				
Master Station				ROUGH IN AND CONNECT ONLY
Substation				ROUGH IN AND CONNECT ONLY
Relay				ROUGH IN AND CONNECT ONLY
Power Supply				
Conduit	EC	EC	EC	Coordinate the exact mount location of devices with EC to ensure that all conduits and back boxes are installed in the optimal locations.
Category 6/IP Wiring	CC	CC	CC	
Non-Category 6/IP Wiring	SC	SC	SC	
Patch panel, patch cords	CC	CC	CC	
Power Over Ethernet POE Extenders	CC	CC	CC	

Fibre optic cable, connectors, patch panel and patch cords	CC	CC	CC	
Intercom System Server complete with: -software, -device licenses, -Integration licenses, -Client computer licenses				ROUGH IN AND CONNECT ONLY
Client Computer with Software				
Electrical circuits, power connections and receptacles	EC	EC	EC	
Video Surveillance (CCTV) System				
Video Surveillance (CCTV) Camera	SC	SC	SC	
Video Surveillance (CCTV) Camera Mount	SC	SC	SC	
Power Supply	SC	SC	SC	
Power Over Ethernet POE Extenders	SC	SC	SC	
Conduit	EC	EC	EC	Coordinate the exact mount location of devices with EC to ensure that all conduits and back boxes are installed in the optimal locations.
Category 6/IP Wiring	CC	CC	CC	
Non-Category 6/IP Wiring	SC	SC	SC	
Patch panel, patch cords	CC	CC	CC	
Fibre optic cable, connectors, patch panel and patch cords	CC	CC	CC	
Network Video Recorder (NVR) complete with: -software, -device licenses, -Integration licenses, -Client computer licenses	SC	SC	SC	
Client Computer with Software	SC	SC	SC	
Electrical circuits, power connections and receptacles	EC	EC	EC	
Security Systems Integration				
Core Switch				BY OWNER
Edge switch				BY OWNER
Firewall				BY OWNER
Keyboard Video Mouse (KVM)	CC	CC	CC	
Communications Cabinet	CC	CC	CC	
Uninterruptable Power Supply (UPS)	CC	CC	CC	
Servers complete with: -software, -device licenses, -Integration licenses, -Client computer licenses	SC	SC	SC	
Conduit	EC	EC	EC	Coordinate the exact mount location of devices with EC to ensure that all conduits and back boxes are installed in the optimal locations.
Category 6/IP Wiring	CC	CC	CC	

Non-Category 6/IP Wiring	SC	SC	SC	
Patch panel, patch cords	CC	CC	CC	
Power Over Ethernet POE Extenders	CC	CC	CC	
Fibre optic cable, connectors, patch panel and patch cords	CC	CC	CC	
Electrical circuits, power connections and receptacles	EC	EC	EC	

1.5. INTENT

- 1.5.1. The Specifications are an integral part of the accompanying Drawings. Any item or subject omitted from one or the other, but which is either mentioned or reasonably implied, is considered as properly and sufficiently specified.
- 1.5.2. Be completely responsible for the acceptable condition and operation of all systems, equipment, and components forming part of the installation or directly associated with it. Promptly replace defective material, equipment, and repair related damages. Ensure that replacement of equipment and repair to damages is coordinated with other trades completed in a timely fashion so as not to affect the complete construction of the Electronic Safety and Security Systems and/or work by others.

1.6. DRAWINGS, CHANGES, AND INSTALLATION

- 1.6.1. The drawings are intended to show the general character and scope of the work and not the exact details of the installation. Ensure that installation is complete with all accessories required for a complete and operative installation.
- 1.6.2. The location, arrangement, and connection of equipment and material as shown on the drawings represent a close approximation to the intent and requirements of the contract. The right is reserved by the Electronic Safety and Security Engineer's Representative to make changes required to accommodate conditions arising during the progress of the work, at no extra cost.
- 1.6.3. Certain details indicated on the drawings are general and specific labeled detail references to each occurrence of use are not indicated, however, such details apply to every occurrence on the drawings.
- 1.6.4. The location and size of existing services shown on the drawings are based on the best available information. Verify the actual location of existing services in the field before commencing work.
- 1.6.5. At no extra cost, make all changes and modifications necessary to ensure coordination and to avoid interference and conflicts with other trades, or to accommodate existing conditions.
- 1.6.6. Leave areas clear where space is indicated as reserved for future equipment, and equipment for other trades.
- 1.6.7. Leave adequate space and provisions for removal of components and servicing of equipment, with minimum inconvenience to the operation of systems.
- 1.6.8. Where equipment is shown to be 'roughed in only' obtain accurate information from the Electronic Safety and Security Engineer's Representative before proceeding with the work.
- 1.6.9. The location of outlets, luminaires, diffusers, grilles, registers, thermostats, sprinklers, and all other equipment shown on drawings (if shown) is diagrammatic.

- 1.6.10. Mark out work and fully coordinate with all other trades. Prepare dimensioned layouts of each room before rough-in for review by Electronic Safety and Security Engineer's Representative. Review with Electronic Safety and Security Engineer's Representative before rough-in. Do not proceed with any work until the Electronic Safety and Security Engineer's Representative has reviewed and approved the layout drawings.
- 1.6.11. Remedy any work not installed in the correct location.
- 1.7. APPROVED EQUAL
- 1.7.1. Wherever the term "or approved equal" and or "approved equivalent" is used herein, it is understood that reference to the specified trade name, brand name, manufacturer's name, model number, and catalogue number has been made solely to indicate the minimum standard of quality required in material, workmanship, and service.
- 1.7.2. Submit shop drawings of proposed equal and or proposed equivalent with bid.
- 1.7.3. The review and acceptance of proposed equals and or proposed equivalents is at the sole discretion of the Owner and their Engineer's Representatives.
- 1.8. SUBSTITUTIONS AND ALTERNATES
- 1.8.1. Proposed substitutions and alternates must include the following:
- .1 Detailed description of proposed substitution including comparative matrix indicating respective functions of items originally specified and the proposed solution
 - .2 Respective costs of items originally specified and the proposed solution
 - .3 Statement of compliance with applicable Building Codes and the requirements of jurisdictional authorities
 - .4 Statement of compliance with the contract drawings specifications and an addenda
 - .5 Affect concerning compatibility with and interface with adjacent building materials and components
 - .6 Reasons for the request.
- 1.8.2. The Electronic Safety and Security Engineer's Representative's decision regarding the acceptance or rejection of the proposed substitution is considered final. Substitutions may be accepted if the delivery of the component or item is such that it does not jeopardize the construction schedule. Otherwise, substitution is not allowed.
- 1.8.3. Submit shop drawings of substitutions with bid.
- 1.9. CONFLICTING REQUIREMENTS
- 1.9.1. In the case of conflict or discrepancy in the requirements indicated in the contract documents the more stringent and/or more onerous requirement apply.
- 1.10. EQUIPMENT AND MATERIALS MINIMUM REQUIREMENTS
- 1.10.1. Ensure that materials and equipment supplied by this Division is new and free from defects.
- 1.10.2. Ensure all equipment and material for which there is a listing service bear a UL/ULC and/or CSA and/or ESA label.
- 1.10.3. Ensure equipment meet all applicable FCC/CRTC Regulations.
- 1.10.4. Ensure materials have a flame spread rating of 25 or less and a smoke-developed rating of 50 or less, following NFPA 255.

1.11. COOPERATION WITH OTHER DIVISIONS

- 1.11.1. Ensure Electronic Safety and Security cabling not touch or be supported from piping, ductwork, conduits, ceiling supports, or any other structure/equipment.
- 1.11.2. Provide all items to be built in ample time for the rapid progress of the work. Schedule and proceed with work as required to satisfy the construction schedule.

1.12. EXISTING SERVICES AND EQUIPMENT

- 1.12.1. Make all changes and connections to existing services in a manner and at a time approved by the Safety and Security Engineer's Representative and/or the Owner to avoid interruption of such services during normal working hours. Ensure changes and connections to existing services is made outside of normal working hours, at no extra cost to the Contract.

1.13. METRIC CONVERSIONS

- 1.13.1. Ensure particular care is taken with imperial versus S.I. metric conversions. This applies to all services including, equipment, material, and site services in both new and existing installations.

1.14. SCHEDULE, ACCESS, PROTECTION, AND CLEAN-UP

- 1.14.1. The construction schedule places restrictions on the duration of construction within areas and the duration of shut-down of equipment. Refer to the General Conditions for all requirements.
- 1.14.2. Refer to the General Conditions and conform to all requirements.
- 1.14.3. Refer to the security and protection requirements in the General Conditions and conform to all requirements. There is no smoking, and the site is kept clean at all times.

1.15. CUTTING, PATCHING, AND REPAIRING

- 1.15.1. Perform all cutting, patching, repair, and making good related to the Electronic Safety and Security Systems work including any penetrations through walls or floors.
- 1.15.2. Allow for all costs associated with cutting, patching, repair, and making good related to the Electronic Safety and Security Systems work including any penetrations through walls or floors.
- 1.15.3. Paint all visible Electronic Safety and Security systems conduit to match existing.
- 1.15.4. Coordinate the colour and location of all conduits, security devices, and their housing with architect and architectural drawings on-site before installation.

1.16. HOISTING FACILITIES

- 1.16.1. Provide all hoisting required to perform all work.

2. Products

2.1. ELECTRONIC SAFETY AND SECURITY SYSTEMS

- 2.1.1. Provide all materials as required for complete turnkey, end-to-end Electronic Safety and Security Systems.
- 2.1.2. Fasteners

- .1 Provide security tamperproof fasteners for all visible exposed devices, equipment, and components in all areas. Coordinate fastener type with the Owner.

3. Execution

3.1. PRODUCT DELIVERY REQUIREMENTS

- 3.1.1. Unload materials from delivery trucks in such a manner as to protect the materials from damage. In particular, reels of the cable is not unloaded by dropping them off the vehicle.

3.2. PROTECTING INSTALLED SYSTEMS AND CONSTRUCTION

- 3.2.1. Be responsible for the assembly of equipment/materials, protection of equipment, and related items until the project cutover. Be responsible for any damage to equipment. All damage is repaired at the Owner's request, the equipment is replaced at no extra charge to the Owner.

3.3. ELECTRONIC SAFETY AND SECURITY SYSTEMS

- 3.3.1. Provide complete turnkey, end-to-end Electronic Safety and Security Systems.

3.4. WARRANTY MAINTENANCE SERVICES

- 3.4.1. Provide a Warranty for the completed work to be free of defects in workmanship and materials for 1years from the date of system acceptance. If the workmanship or materials is found to be defective or not following the contract documents during the warranty period, correct it promptly with factory-certified technicians at no cost. Provide all labor and materials to facilitate correction.
- 3.4.3. Ensure warranty covers all installation for the Electronic Safety and Security Systems including all hardware, hardware configurations, software, software configurations, wiring/cabling, conduit, pathways, and all active and passive components.
- 3.4.4. Provide maintenance at no extra cost during the warranty period. The maintenance include:
 - .1 Execute system health check every 6 months during the warranty period on all systems components including devices, cabling all passive and active hardware all software, and firmware. Correct all defects and make all corrections to components and software to ensure the entire system is functioning optimally and according to the manufacturer's recommendations.

3.5. GENERAL REQUIREMENTS

- 3.5.1. Provide all services required and equipment necessary to maintain all operations of the installed Electronic Safety and Security Systems during the period of the warranty.

3.6. SOFTWARE

- 3.6.1. Provide all available software and firmware updates during the period of the warranty and verify operation in the system. Ensure all updates are accomplished on time, fully coordinated with the Owner's representatives, include training for the new changes/features enabled, and incorporated into the operations and maintenance manuals, and software documentation.

3.7. DESCRIPTION OF WORK

- 3.7.1. Provide respective systems manufacturer's required scheduled and unscheduled maintenance and all other work necessary to keep the system at its maximum performance.

3.8. PERSONNEL

- 3.8.1. Ensure Service personnel are factory certified in the maintenance and repair of the system equipment installed under this specification. The Owner is advised in writing of the name of the designated service representative, and any change in personnel.

3.9. RECORDS AND LOGS

- 3.9.1. Maintain records and logs of each task performed. Organize cumulative records for each component and the complete system chronologically. A continuous log is maintained for all devices. The log contain all initial settings. Complete logs is kept and available for inspection on-site, demonstrating that planned and systematic adjustments and repairs have been accomplished.

3.10. WORK REQUESTS

- 3.10.1. Record separately each service call request on a service request form. The form include the model and serial number identifying the component involved, its location, date and time the call was received, specific nature of the trouble, names of service personnel assigned to the task, instructions describing what has to be done, the amount and nature of the materials used, the time and date work started, and the time and date of completion. Deliver a record of the work performed within five (5) days after work is accomplished.

3.11. SYSTEM MODIFICATIONS

- 3.11.1. Make any recommendations for system modification in writing to the Owner. No system modifications is made without prior approval of the Owner. Any modifications made to the system make sure it is incorporated into the operations and maintenance manuals, and other documentation affected.

END OF SECTION

28 01 01.00 Operation and Maintenance of Electronic Safety and Security

1. General

1.1. TRAINING

- 1.1.1. Include for adequate training of a minimum of 4 operations personnel on the operation and maintenance of the Electronic Safety and Security Systems. The training is a minimum of eight (8) hours of instruction in two (2) 4-hour segments.
- 1.1.2. Coordinate with the Owner to configure and or reconfigure and populate and or repopulate all Electronic Safety and Security system-related databases, configure and or reconfigure all the systems parameters to the Owners' satisfaction, until initial databases are complete and functional, and until all the security system parameters are working to the Owners satisfaction. Provide one technician to work side-by-side with the Owner's representatives to assist and instruct the Owner's representatives with further customization of all systems functionalities to the Owner's satisfaction.
- 1.1.3. The training includes oral and written presentations and onsite system interactive training sessions that ensure operational competency of operations personnel on each Electronic Safety and Security system.
 - .1 Provide an electronic copy of maintenance manuals and operating instructions. This include comprehensive descriptive datasheets, brochures, and technical manuals for all systems and equipment forming part of the contract. Ensure that the manuals include wiring and schematic diagrams for the Electronic Safety Security System and all related subsystems.
 - .2 For each Electronic Safety and Security subsystem, Provide an A4 laminated sheet with short-form operating instructions on one side, and a site diagram showing systems components on the other.
 - .3 Submit a full schedule of maintenance that is carried out on each Electronic Safety and Security system during the warranty period and under subsequent maintenance contracts.
- 1.1.4. Training covers all aspects of all the systems under the electronic safety and security scope.
- 1.1.5. Record the training sessions on video with suitable audio enhancement. Provide systems manufacturer's training videos and recorded training sessions in digital format that can be viewed on a commercially available media player and edited for future training sessions. Submit all video files via secure file transfer.

2. Products

2.1. NOT USED

3. Execution

3.1. NOT USED

END OF SECTION

28 05 00.00 Common Work Results for Electronic Safety and Security

1. General

1.1. FLOOR/CEILING TILES

- 1.1.1. Allow for the removal and re-installation of all floor/ceiling tiles in areas affected by work. This is done daily for all areas that are occupied during the construction period. Otherwise, remove and re-install the tiles after work is complete.
- 1.1.2. Replace all soiled and or damaged ceiling tiles during the installation of any work described in this document. Damages include chipping, breaking, or fingerprints. Final decisions on the trade responsible for any damage to ceiling tiles is made by the Project Manager and/or the Electronic Safety and Security Engineer's Representative.
- 1.1.3. Store and protect all floor/ceiling tiles when they have been removed from the floor/ceiling grid.

1.2. SAFETY OF PERSONS AND PROPERTY

- 1.2.1. Comply with all laws, ordinances, rules, regulations, policies of the Owner, and lawful orders of any public authority having jurisdiction for the safety of persons or property or to protect them from damage, injury or loss.
- 1.2.2. Moderate public pedestrian traffic should be expected around all work locations. Ensure Ladders scaffold, installation materials, and all other hazardous conditions are fully protected at all times. Warning cones, signs, barricades, and warning tapes is used to warn and protect persons and property at all times in public corridors.
- 1.2.3. Ensure that the work done does not interfere with legal fire exits. Corridors, areas of egress, fire protection standpipes, hydrants, and exit stairs is maintained at all times.
- 1.2.4. No open flames/smoking permitted without the prior written approval of the Owner.
- 1.2.5. Set up and remove all signage and safety measures to ensure that other trades and non-trade personnel are safe from all work being performed.

1.3. ACCESS TO SITE

- 1.3.1. Coordinate site access with the General Contractor and Owner as determined during the initial project meeting.

1.4. IDENTIFICATION

- 1.4.1. All personnel are identified by either uniform or company ID. In addition, wear Owner provided ID for required card access locations or identification. All Owner ID must be returned daily or at the end of the project as determined by the Owner.

1.5. EMERGENCY FACILITIES

- 1.5.1. Maintain at all times free access to fire lanes and emergency and utility control facilities such as fire alarm boxes, utility vaults, manholes, and junction boxes.

1.6. PRODUCT DELIVERY REQUIREMENTS

- 1.6.1. Allow for complete delivery, handling, and installation of all materials used in the performance of the work.
- 1.6.2. Arrange for the delivery of Owner furnished equipment/materials related to this Specification and related items, including unloading of supplier's truck, elevator scheduling, and placement on Owner premises as indicated on Contract Drawings.

1.7. PRODUCT AND TOOLS STORAGE REQUIREMENTS

- 1.7.1. Allow for complete storage and handling of all materials used in the performance of the work.
- 1.7.2. Storage of job boxes on the site during construction may be allowed by the Owner. Coordinate the storage of job boxes onsite with the Owner. The Owner and his representatives are in no way responsible for any stored tools and or materials.

1.8. CONFINED SPACES

- 1.8.1. Comply with all code-related and Owner specific safety requirements when performing work in a confined space.

1.9. CO-ORDINATION WITH OCCUPANTS

- 1.9.1. Coordinate all work with the Owner/tenant of the floor space for daily work.

2. Products

2.1. NOT USED

3. Execution

3.1. PRODUCT DELIVERY REQUIREMENTS

- 3.1.1. Unload materials from delivery trucks in such a manner as to protect the materials from damage. Ensure reels of cable are not unloaded by dropping them off the vehicle.

3.2. PROTECTING INSTALLED SYSTEMS AND CONSTRUCTION

- 3.2.1. Assemble the above equipment/materials and protect the above equipment and related items until the project cutover. Replace all damaged equipment at no extra charge.

END OF SECTION

28 05 03.00 Record Drawings

1. General

1.1. NOT USED

2. Products

2.1. RECORD DRAWINGS

2.1.1. Request in writing from the Engineer's Representative all Contract Drawings in native drawing file format (AutoCAD, Revit, .pdf, etc.) required to complete the Record Drawings. Complete the attached form and pay the Engineer's Representative directly the costs identified within the form before receiving the Contract Drawings. After the final Record Drawings have been reviewed, provide a copy of the drawings via secure file sharing utility. Provide a copy to the Engineer's Representative for their records and a copy with each set of operation and maintenance manuals. Provide additional copies if required under the General Conditions. Use the latest release of the native drawing file format software.

2.1.2. The Record Drawings include:

- .1 native drawing file format and .pdf copies of Site and Floor Plans indicating locations of all devices
- .2 native drawing file format and .pdf copies of Point-to-point wiring schematics of all systems and subsystems
- .3 native drawing file format and .pdf copies of Elevations of all rack, cabinets, and backboard showing details device mounting
- .4 MS Word/Excel and .pdf copies of All related schedules
- .5 MS Word/Excel and .pdf copies of Testing and commissioning documentation for all devices

2.1.3. Identify the cost of Record Drawings and the Operation and Maintenance Manuals as a separate line item on progress draw. The following values are to be broken out:

\$3,500	For Contracts up to \$250,000
2% of Contract	For Contracts from \$250,000 to \$1,500,000

2.1.4. The project remains incomplete and no money is released until the final electronic versions of Commissioning Test Results, As-built Drawings and Operations and Maintenance Manuals are received.

2.1.5. Ensure that Final Record Drawings does not contain markings or corrections by hand (i.e. marker, pen, pencil, etc.). References to the Architect and Engineer must be deleted from the drawings.

2.1.6. Ensure that Final Record Drawings include all revisions made to the drawings during construction, including all approved changes. The Record Drawings also include the routing of all feeders except for branch circuits. Include slab layout drawings in the as-built drawing package.

2.1.7. Drawings Requirements:

- .1 Ensure all Record Drawings are prepared using the Owner's drawings standards. Obtain the Owner's drawing standards from the Owner before preparing Record Drawings
 - .2 All files must accompany a complete list of layer names and a brief description of each layer's use.
 - .3 Final Record Drawings drawings are returned via secure file transfer.
 - .4 Each file is dated and named with Engineer's Representative and Owner, Contract number, file names, and Drawing number.
 - .5 Ensure all drawings are in the same units as issued on Bid Documents.
 - .6 Provide a complete list of symbols (block) names with a description of each symbol.
 - .7 Special effort is made to ensure that drafting is accurate: i.e. appropriate lines are indeed horizontal and vertical; lines that should intersect do but not over-intersect and ensure that entities are placed on correct layers.
- 2.1.8. Maintain hard or electronic copy of drawings on-site on which mark as the job progresses, all changes and deviations from that shown on Contract Drawings.
- 2.1.9. On completion of the building, forward to the Engineer's Representative electronic copy of final drawings indicating all such changes and deviations for review by the Engineer's Representative.
3. Execution
- 3.1. NOT USED

Project Name: _____

attention: _____

Project No.: _____ Date: YYYY-MM-DD Issued by: _____

Conditions for Limited Use of Drawings

Authorization for limited use of the drawing files listed below is hereby granted, subject to the following conditions. The signing of this form constitutes acceptance and agreement with the conditions and limitations.

Copyright is reserved. The drawing and design contained in the drawing file is at all times the exclusive property of the Architect/Engineer and is not be used without the Architect/Engineer's written consent.

The drawing file may not be used wholly or in part for any purpose other than the intended use as stated on this form. Copying or distribution of this drawing file in whole or in part to parties other than those signing below is not allowed.

The file represents drawings that were prepared primarily to obtain tender prices. The drawings may or may not incorporate subsequent revisions, change orders, or addenda that have modified the drawings. files obtained from different disciplines may not be fully updated and coordinated with other disciplines and must be verified from the tender documents. The Architect/Engineer assumes no liability for errors or omissions in the drawing files. The authorized user assumes all risk and expense associated with the use of the drawing files in the production of his work.

References to the Architect and Engineer must be deleted from the drawings.

Please indicate a P.O. Number for charges associated with administrative costs to provide requested drawings.

Our charges are as follows:	\$50.00 each for the first 5 drawings			
	\$20.00 for each additional drawing from 6 to 19			
	\$500.00 for 20 drawings or more			
List of requested drawings:				
Total No. of Drawings:		Total Charge:		+ GST or HST, as applicable

Intended use (Shop drawings, As-built drawings, Installation and Interference drawings, etc.) _____

E-mail (please provide e-mail address) _____

Email address to have a link sent to (one-time download). A cheque in the above amount to be payable to Smith + Andersen or indicate the PO information below. Please sign and email this form to the sender or info@smithandandersen.com acknowledging the above charges and Conditions for Limited Use of Drawings

Accepted by: _____

Signature

Name (print or type)

Company Name

P.O. #

Company Address

Phone #

c.c. Accounting; (Project Principal) – Smith + Andersen

END OF SECTION

28 05 04.00 Submittals – Shop Drawings

1. General

1.1. NOT USED

2. Products

2.1. SUBMITTALS/SHOP DRAWINGS

2.1.1. Submittals/Shop Drawings indicate the materials and/or equipment being supplied, all details of construction, accurate dimensions, capacity, operating characteristics, and performance. Each Shop Drawing give the identifying number of the specific assembly for which it was prepared (e.g. B-P2-AAA).

2.1.2. All shop drawings identify the specific model number of equipment being supplied.

2.1.3. Each Shop Drawing for non-catalogue items is prepared specifically for this project. Shop Drawings data sheets and brochures for catalogue items are marked clearly to show the items being supplied.

2.1.4. Each Shop Drawing or catalogue sheet is stamped and signed to indicate that the shop drawing has been checked for conformance with all requirements of the contract drawings and specifications, that all proposed materials have been coordinated with other equipment to which it is attached, and/or connected and that all dimensions have been verified to ensure the proper installation of equipment within the available space and without interference with the work of other trades. Ensure that all electrical, mechanical, and architecture coordination are complete before submitting drawings for review.

2.1.5. Shop Drawings include:

- .1 Table of content
- .2 Video surveillance system storage calculations
- .3 Video surveillance camera field of view calculations
- .4 Door hardware coordination schedules
- .5 For each product catalogue datasheets provided, highlight and mark the exact model number including all options of each propose product.
- .6 Detailed schematic riser drawings indicating the physical and logical connectivity of each system and how each product is implemented in the physical and logical connectivity of each system.
- .7 A system narrative explaining the physical and logical connectivity of each system as well as the functionality of each system.
- .8 Detailed floor plan drawings with a legend indicating the location of each device that is installed.
- .9 An itemized shop drawing index with a summary list of items being submitted for review. The list to indicate Item Number, Item Manufacture and Model Number and Item name and a Review Comments Column.
- .10 Testing and commissioning plans
- .11 Training Plans

- .12 Manufacturer certifications
- .13 All additional requested information as determined by the Engineer's Representative

3. Execution

- 3.1.1. Submit all shop drawings as a single complete package.
- 3.1.2. Submit all submittals/shop drawings electronically in PDF format. Submittal is complete with a transmittal bound to the PDF file with the transmittal identifying the total number of pages in the submittal including the transmittal page.
- 3.1.3. Ensure that installation of any equipment does not start until after the Engineer's Representative has reviewed Shop Drawings.
- 3.1.4. When requested, Shop Drawings is supplemented by data explaining the theory of operation
- 3.1.5. Provide space for Shop Drawing review stamps for Engineer's Representative. This space is clear of all technical information and is not on the back of any sheets.
- 3.1.6. One original Shop Drawing is returned electronically.

END OF SECTION

28 05 05.20 Definitions and Abbreviations

1. General

1.1. DEFINITIONS

1.1.1. Generally, the following definitions are used in this Division:

Addendum	-	Normative document used to provide additional requirements and recommendations to a published document (e.g., standards, contracts). When published, an addendum effectively becomes part of the document that it supports.
Bonding	-	The permanent joining of metallic parts to form an electrically conductive path that will ensure electrical continuity and the capacity to conduct safely any current likely to be imposed.
Bonding Conductor (BC)	-	A conductor is used specifically for bonding.
Building Entrance Facility	-	The room or space inside a building where telecommunications cables enter and leave the building.
Central Management Station	-	A personal computer device that is complete with Operating system software and Systems specific client and or server software. The Central Management Station is used to configure, monitor and manage electronic safety and security systems.
Change Notice	-	Normative document approved to provide additional requirements and recommendations that describe and authorize the implementation of an engineering change to the product and its approved configuration documentation.
Contemplated Change Notice	-	Normative document to provide additional requirements and recommendations that describes the implementation of an engineering change to the product and its approved configuration documentation for pricing. This document does not authorize the implementation of a change to the product and its approved configuration documentation.
Cut Over	-	The live date(s) when the Owner will occupy the space as indicated by date and/or phasing.
Contract Documents	-	All Electronic Safety And Security Systems / Security, Electrical, Architectural, Mechanical and Structural Drawings and specifications and schedules issued about this project including any future changes and revisions of said documents.
Contract Drawings	-	All Electronic Safety And Security Systems / Security, Electrical, Architectural, Mechanical and Structural Drawings issued about this project including any future changes and revisions of said documents.
Grounded Conductor	-	A system or circuit conductor that is intentionally grounded.
Grounding System	-	A system of hardware and wiring that provides an electrical path from a specified location to an earth-ground point.
Owner	-	The person "in charge" of the overall project
Project	-	Supply and installation of a complete Integrated Electronic Safety and Security Systems as described in this document.
Provide	-	Supply, install and configure as per contract documents.
Shop Drawing	-	Drawings, diagrams, illustrations, schedules, performance charts, and other data prepared to illustrate how specific portions of the work is installed. This includes point to point high-level integration diagram, riser diagram, termination diagram, panel layout, door types, and product datasheet.

1.2. ABBREVIATIONS

1.2.1. Generally, the following abbreviations are used in this Division:

A	-	Ampere
ac	-	Alternating current
ACR	-	Attenuation to Cross-Talk Ratio
ADC	-	Analogue to Digital Converter
A/E	-	Architect or Engineer
AFF	-	Above Finished Floor
AHJ	-	Authority Having Jurisdiction
AME	-	Architectural, Mechanical, Electrical
ANSI	-	American National Standards Institute
AP	-	Access Point
ASCII	-	American Standard Code for Information Interchange
ASTM	-	American Society for Testing and Materials
ATD	-	Asynchronous Time Division
ATDM	-	Asynchronous Time Division Multiplexing
ATM	-	Asynchronous Transfer Mode
Attn	-	Attenuation
AV	-	Audiovisual
AWG	-	American Wire Gauge
BAS	-	Building Automation System
BC	-	Bonding Conductor
BCD	-	Backbone Conduit
BCT	-	Bonding Conductor for Telecommunications
BEF	-	Building Entrance Facility
BER	-	Bit Error Rate
BERT	-	Bit Error Rate Test
BFOC	-	Bayonet Fibre Optic Connector
BIC	-	Building Industry Consultant
BICSI®	-	Building Industry Consulting Service International
bit	-	Binary Digit
BOM	-	Bill Of Material
b/s	-	Bit per Second
BWA	-	Broadband Wireless Access
CA	-	Cable
CAD	-	Computer Aided Design
CATV	-	Community Antenna Television (Cable Television)
CCIA	-	Computer Communications Industry Association
CCN	-	Contemplated Change Notice
CD	-	Compact Disc
CD	-	Change Directive (same as Change Notice and Change Order)
CEC	-	Canadian Electrical Code
cm	-	Centimetre
CMP	-	Communications Plenum
CMR	-	Communications Riser
CN	-	Change Notice (same as Change Directive and Change Order)
CO	-	Change Order (same as Change Notice and Change Directive)
coax	-	Coaxial Cable
CP	-	Consolidation Point
CPU	-	Central Processing Unit

CPVC	-	Chlorinated Polyvinyl Chloride
CSA	-	Canadian Standards Institute
CSC	-	Construction Specifications Canada
CSI	-	Construction Specifications Institute
CT	-	Cable Tray
Cu	-	Copper
c/w	-	Complete With
dB	-	Decibel
dB/km	-	Decibel per Kilometre
dBm	-	Decibel milliwatt
dBmV	-	Decibel millivolt
demarc	-	Demarcation Point
DSL	-	Digital Subscriber Line
EF	-	Entrance Facility
EIA	-	Electronics Industry Alliance
ELFEXT	-	Equal Level Far-End Crosstalk
ESSS	-	Electronic Safety and Security System/s
e-mail	-	Electronic Mail
EMI	-	Electromagnetic Interference
EMI/RFI	-	Electromagnetic Interference / Radio Frequency Interference
ER	-	Equipment Room
ESD	-	Electrostatic Discharge
e/w	-	Equipped With
FC	-	Fibre Connector
FCC	-	Federal Communications Commission
FOV	-	Field Of View
ft	-	Foot / Feet
ft ²	-	Square Foot / Feet
G	-	Giga
Gb	-	Gigabit
GB	-	Gigabyte
Gb/s	-	Gigabit per Second
GC	-	General Contractor
GHz	-	Gigahertz
HC	-	Horizontal Cross-connect
Hz	-	Hertz
I	-	Current
IC	-	Intermediate Closet
IC	-	Intermediate Cross-connect
ID	-	Identification
ID	-	Inside Diameter
IDC	-	Insulation Displacement Connection
IDC	-	Insulation Displacement Connector
IDC	-	Insulation Displacement Contact
IDF	-	Intermediate Distribution Frame
IEEE®	-	Institute of Electrical and Electronics Engineers, Inc.®
IG	-	Isolated Ground
in	-	Inch
in ²	-	Square Inch
I/O	-	Input / Output (Device)

IOR	-	Index Of Refraction
IP	-	Internet Protocol
ISDN	-	Integrated Services Digital Network
ISO	-	International Organization for Standardization
IT	-	Information Technology
kb	-	Kilobit
kB	-	Kilobyte
kg	-	Kilogram
km	-	Kilometre
kV	-	Kilovolt
kVA	-	Kilovoltampere
kW	-	Kilowatt
kWh	-	Kilowatt hour
LAN	-	Local Area Network
laser	-	Light Amplification by Stimulated Emission of Radiation
lb	-	Pound
LED	-	Light Emitting Diode
LO	-	Laser Optimized
LSZH	-	Low Smoke Zero Halogen
m	-	Metre
m ²	-	Square Metre
mA	-	Milliampere
MAC	-	Move, Add, or Change
MAN	-	Metropolitan Area Network
Mb	-	Megabit
MB	-	Megabyte
Mb/s	-	Megabit per Second
MB/s	-	Megabyte per Second
MC	-	Main Cross-connect
MDF	-	Main Distribution Frame
MGB	-	Main Grounding Busbar
MHz	-	Megahertz
mi	-	Mile
min	-	Minute
mm	-	Millimetre
MM	-	Multimode
MMF	-	Multimode Fibre
MPP	-	Modular Patch Panel
ms	-	Millisecond
MSDS	-	Material Safety Data Sheet
MW	-	Megawatt
NBCC	-	National Building Code of Canada
NESC	-	National Electrical Safety Code
NIC	-	Network Interface Card
NRCC	-	National Research Council of Canada
OD	-	Outside Diameter
OEM	-	Original Equipment Manufacturer
OF	-	Optical Fibre
OSDP		Open Supervised Device Protocol
PDU	-	Power Distribution Unit

PIR	-	Passive Infrared
PSACR	-	Power Sum Attenuation to Crosstalk Ratio
PSELFEXT	-	Power Sum Equal Level Far-End Crosstalk
PSNEXT	-	Power Sum Near-End Crosstalk
PSP	-	Physical Security Professional
PTZ	-	Pan Tilt Zoom
PVC	-	Polyvinyl Chloride
QA	-	Quality Assurance
QC	-	Quality Control
QoS	-	Quality of Service
Qty	-	Quantity
RCDD®	-	Registered Communications Distribution Designer
RF	-	Radio Frequency
RFI	-	Radio Frequency Interference
RJ	-	Registered Jack
rms	-	Root Mean Square
RU	-	Rack Unit (1.75")
RX	-	Receive
RX	-	Receiver
SAN	-	Storage Access Network
SC	-	Single Fibre Coupling Optical Fibre Connector
SCC	-	Standards Council of Canada
SCS	-	Structured Cabling System
ScTP	-	Screened Twisted Pair
SFTP	-	Screened Foiled Twisted Pair
SI	-	International System of Units (Le Système International d'Unités)
SLA	-	Service level Agreement
SM	-	Singlemode
SMF	-	Singlemode Fibre
SNMP	-	Simple Network Management Protocol
SNR	-	Signal-to-Noise Ratio
STP	-	Shielded Twisted Pair
STP-A	-	Shielded Twisted Pair A
TBB	-	Telecommunications Bonding Backbone
TBBIBC	-	Telecommunications Bonding Backbone Interconnecting Bonding Conductor
TC	-	Telecommunications Closet
TDD	-	Telecommunications Device for the Deaf
TGB	-	Telecommunications Grounding Busbar
TGR	-	Telecommunications Grounding Rod
TIA	-	Telecommunications Industry Association
TMGB	-	Telecommunications Main Grounding Busbar
TP	-	Twisted Pair
TR	-	Telecommunications Room
TS	-	Technical Standard
TSB	-	Telecommunications Systems Bulletin (formerly Technical Systems Bulletin)
TTY	-	Teletypewriter / Text Telephone
TV	-	Television
TX	-	Transmit

TX	-	Transmitter
UD	-	Underfloor Duct
UL®	-	Underwriters Laboratories Inc.®
ULC	-	Underwriters Laboratories of Canada
UPC	-	Universal Product Code
UPS	-	Uninterruptible Power Supply
UTP	-	Unshielded Twisted Pair
V	-	Volt
VA	-	Volt-Ampere
VLAN	-	Virtual Local Area Network
VoIP	-	Voice over Internet Protocol
VPN	-	Virtual Private Network
W	-	Watt
WAN	-	Wide Area Network
WAP	-	Wireless Application Protocol
WiFi	-	Wireless Fidelity
Wi-Fi	-	Wireless Fidelity
WLAN	-	Wireless Local Area Network
WMAN	-	Wireless Metropolitan Area Network
WWAN	-	Wireless Wide Area Network

2. Products

2.1. NOT USED

3. Execution

3.1. NOT USED

END OF SECTION

28 05 13.00 Conductors and Cables for Electronic Safety and Security

1. General

1.1. WORK INCLUDED

- 1.1.1. All Electronic Safety and Security Systems conductors and cables is installed in pathways as shown on contract drawings. Pathways include conduit, cable trays, and cable troughs.
- 1.1.2. Provide conductors and cables as detailed in Contract Documents and as required and as specified by the manufacturer to ensure proper operation of all devices and systems. Use pathways to distribute the cables throughout the facility. Where the cables leave the pathways provided by Div 26 and extend to the termination point provide conduit as needed to support and secure the cables.
- 1.1.3. Where pathways are not provided by Division 26 and are required as noted on drawings and in this specification provide pathways for all Electronic Safety and Security Systems conductors and cables.
- 1.1.4. Avoid scraping, denting, or otherwise damaging cables, before, during, or after installation. Without any additional compensation replace damaged cables.
- 1.1.5. Ensure that all cable lengths are sufficient to allow for horizontal and vertical runs, wastage, connectorization, and future moves.

1.2. CABLE ROUTING

- 1.2.1. Make any necessary changes or additions to the routing of cables, pathways to accommodate structural, mechanical, electrical, and architectural conditions. Where pathways or cables are shown diagrammatically run them parallel to grid lines. If it is necessary to run cables otherwise to accommodate acceptable cable lengths, written permission must be obtained from the Electronic Safety and Security Engineer's Representative before installation.

2. Products

2.1. CABLING

- 2.1.1. Conductors and cables are to be CMR where installed completely in conduit or where installed in non-plenum rated areas. Conductors and cables are to be CMP where not completely installed in conduit or installed in plenum-rated areas. All cables conform to the recommendations of the manufacturers of the electronic safety and security systems.
- 2.1.2. Approved Manufacturers:
 - .1 Belden
 - .2 CommScope
 - .3 Hubbell
 - .4 Leviton
 - .5 Panduit
- 2.1.3. Conductors and cables are outdoor-rated where installed outdoor or installed in locations where they will be exposed to weather elements.

- 2.1.4. Conductors and cables are rated for the environment and or environments in which they are being installed.
- 2.1.5. Provide and install shielded cables where required and or recommended by the manufacturer of the electronic safety and security systems.
- 2.1.6. The cabling shown is for typical systems. All cabling is as required and specified by the manufacture of the electronic safety and security systems.
- 2.1.7. All wiring is of the proper gauge, type, and quantity of conductors as required and as specified by the manufacturer to ensure proper operation of electronic safety and security systems and peripheral devices.
- 2.1.8. Multiconductor cables have the conductors colour-coded.
- 2.1.9. Ensure all conductors and cables are CSA approved and is be stamped accordingly.
- 2.1.10. Card Readers: Minimum 3 pair, AWG 22, overall shielded or as required by the manufacturer
- 2.1.11. Door contact (magnetic contact): Minimum 4 conductor, AWG 22 or as required based on distance from the controller
- 2.1.12. Motion request to exit devices: Minimum 4 conductor, AWG 22 as required based on distance from the controller
- 2.1.13. Electric strikes, magnetic locks, electric latches, electric mortise locks, and all other electrified locks: Minimum 4 conductor, AWG 18 or as required based on distance from the power source
- 2.1.14. Push button and latch bolt monitor request to exit devices: Minimum 4 conductor, AWG 22 as required based on distance from the controller
- 2.1.15. Motion detector: Minimum 4 conductor, AWG 22 as required based on distance from the controller
- 2.1.16. Glass break detector: Minimum 4 conductor, AWG 22 as required based on distance from the controller
- 2.1.17. Increase conductor quantities and or sizes beyond the above-stated minimums as required to facilitate the proper and complete operation of each respective device and system.
- 3. Execution
 - .1 CABLE DISTRIBUTION
 - 3.1.2. Where cables are not installed in conduit neatly bundle and tie-wrap all cables using Velcro straps.
 - 3.1.3. Follow proper installation and termination practices for all cables. Do not kink or exceed the cable minimum bend radius. Maintain a minimum of four (4) times cable diameter as bend radii if the manufacturer specifies no bend radius.
 - 3.1.4. When bundling cables, comply with the manufacturer's specified bundling practices for installation. Ensure that excess pressure is not placed on the cable at any point that may result in the compression or deformation of the cable jacket and internal pair/conductor geometry.

- 3.1.5. Do not exceed the copper cable's maximum tensile rating during installation. Monitor tension of the cable during installation. Use a dynamometer to record installation tension. Use a tension limiting device to prevent the exceeding of maximum pulling tension specifications during installation. The tension limit is set at or below the manufacturer's limit. Ensure the cable is taken up at intermediate pulling points with an intermediate take-up device as approved by the Electronic Safety and Security Engineer's Representative, to prevent over tension on the cable.
- 3.2. CONDUCTORS AND CABLES
- 3.2.1. Provide all wiring as required for the proper operating of each electronic safety and security system and each peripheral device.
- 3.2.2. Provide and install metal wiring duct to facilitate proper organization and proper dressing of all cables at and around each electronic safety and security system panel.
- 3.2.3. Provide metal wiring duct from conduit endpoints to and around all control panels.
- 3.2.4. All wiring ducts is installed such that the ducts house, protect, and facilitate the routing of all cables at 90-degree angles to and around all access control panels.
- 3.2.5. Provide non-metallic wiring ducts within all control panels to manage all wiring to termination points.
- 3.2.6. All wiring duct is sized to house all cables while maintaining the manufacturer's specified bend radius.
- 3.2.7. Provide all fitting for all wiring duct as required, including; couplings, end caps, brackets, etc.
- 3.2.8. After installation, and before termination, ensure all wiring and cabling is checked and tested to ensure there are no grounds, opens, or shorts on any conductors or shields. A V.O.M. is utilized to accomplish these tests and a reading of greater than 20 Megohms is required to complete the test. All Category 6 and Category 6A cables is tested to EIA/TIA standards.
- 3.2.9. Visually inspect wire and cable for faulty insulation before installation. Protect cable ends at all times with acceptable end caps except during actual termination.
- 3.2.10. Protect wire and cable from kinks.
- 3.2.11. Provide grommets and strain relief where required.
- 3.2.12. Comply with controller and peripheral device manufacturer's installation and termination recommendation.

END OF SECTION

28 05 26.00 Grounding and Bonding for Electronic Safety and Security

1. General
 - 1.1. WORK INCLUDED
 - 1.1.1. Applicable Codes & Standards
 - 1.1.2. Provide grounding & bonding following good industry practices and following the following Codes and Standards:
 - .1 CSA Standard C22.2 No.41 latest version – Grounding & Bonding Equipment
 - .2 CSA Standard T527 (ANSI/TIA/EIA-607-C)
 - .3 CSA Standard T 530-99 - Telecommunications Pathways and Spaces
 - .4 ANSI/EIA/TIA-942-B – Telecommunications Infrastructure Standard for Data Centers
 - .5 Local Codes & Bylaws
 - .6 BICSI requirements
 - 1.1.3. Refer to Electrical Specifications for Electrical Codes and Building Codes.
 2. Products
 - 2.1. GROUNDING & BONDING INFRASTRUCTURE
 - 2.1.1. Rack Grounding Strips
 - .1 Panduit Part# RGS134-1Y or approved equivalent
 - 2.1.2. Rack Jumper Kits
 - .1 Panduit Part# ACG24K or approved equivalent
 - 2.1.3. Thread forming screws
 - .1 Panduit Part # RGTS-CY or approved equivalent
 - .2 Panduit RGTSM6-C or approved equivalent
 - 2.1.4. Bonding screws
 - .1 Panduit Part# RGTBS-C or approved equivalent
 - .2 Panduit RGTBSM6-C or approved equivalent
 - 2.1.5. Provide a green jacketed #6 AWG Stranded Copper Conductor to bond the grounding system to all:
 - .1 Cabinets
 - .2 Racks
 - .3 Metallic Pathways including Cable Tray, Conduit, etc.
 - .4 Metallic sheath of all shielded cables (use cable manufacturer's recommended bond clamp)
 - .5 Metallic enclosures including equipment and controller enclosures, building entrance protection panels, etc.

3. Execution

3.1. GENERAL

- 3.1.1. Confirm existing ground bus in each communications room.
- 3.1.2. Coordinate location of new ground bus in communications rooms.
- 3.1.3. Ground and or Bond all metal components of the Electronic Safety and Security Systems per all applicable codes and standards.
- 3.1.4. Provide, test, label, and document all grounding and bonding cables and related terminations.
- 3.1.5. Ensure that complete metal-to-metal contact is made when grounding to painted or powder-coated metal surfaces.
- 3.1.6. Where Grounding & Bonding Infrastructure is provided Ensure that the Grounding & Bonding Infrastructure does not interfere with, impede and or reduce the integrity of existing grounding systems and practices.

END OF SECTION

28 05 28.00 Pathways for Electronic Safety and Security

1. General

1.1. WORK INCLUDED

- 1.1.1. Where cables leave the pathways, provide cable slings and/or j-hooks to support cabling up to point of termination.

1.2. CABLE DISTRIBUTION

- 1.2.1. Utilize all indicated and available cable pathways such as conduits, Communications cable tray, ducts, surface raceways, and furniture system channels except where otherwise noted.
- 1.2.2. Inside buildings minimize any possibilities of disruption by maintaining the following minimum clearances from electrical and heat sources when routing cables.

Item	Minimum Separation Distances		
	(<2kVA)	(2-5kVA)	(>5kVA)
Unshielded power lines or electrical equipment in proximity to open or non-metallic pathways.	127 mm (5" (in))	305 mm (12" (in))	610 mm (24" (in))
Unshielded power lines or electrical equipment in proximity to a grounded metal conduit pathway.	64 mm (2.5" (in))	152 mm (6" (in))	305 mm (12" (in))
Power lines are enclosed in a grounded metal conduit (or approved equivalent shielding) in proximity to a grounded metal conduit pathway.	---	76 mm (3" (in))	152 mm (6" (in))
Motors	1.2 m (4'-0")		
Transformers	1.2 m (4'-0")		
Fluorescent Luminaires	300 mm (12")		
Pipes (gas, oil, water, etc.)	120 mm (5")		
HVAC (equipment, ducts, etc.)	152 mm (6")		

2. Products

2.1. NON-CONTINUOUS CABLE SUPPORT

- 2.1.1. Provide cable support for the distribution of horizontal and backbone cables where conduit or ladder tray has not been provided.
- 2.1.2. Ensure the size of J-hooks/support suit the number of cables in runs used for distribution.
- 2.1.3. Include any other miscellaneous hardware (angled hanger bracket, hammer/screw-on clamps) required to support horizontal and backbone cabling.

2.2. VELCRO STRAPS

- 2.2.1. Provide Velcro straps. Only Velcro straps is acceptable. Under no circumstance plastic tie-wraps be used.

2.3. GROUNDING WIRE

- 2.3.1. Provide #6 AWG green grounding wire for all metallic components that is grounded and Code Conductor Two Hole Long Barrel with Window Lug to bond the conductor to the ground bus.

3. Execution

3.1. CABLE DISTRIBUTION

- 3.1.1. Exercise caution when pulling cables in pathways to avoid damage to any existing cables.
3.1.2. Follow the manufacturer's maximum pull-force and minimum bend radii.
3.1.3. All cables and components installed and terminated following applicable Codes, Standards, and Regulations.

3.2. CABLE SUPPORT

- 3.2.1. Hangers installed at 1219mm (48") intervals (maximum). Cables run such that sag between supports does not exceed 100 mm (4"). Secure all cables to J-hooks/supports with Velcro straps. Cables combed and dressed for all visible portions of the install. The above-noted conditions are strictly checked. Comb and redress any cables that are unsatisfactory at no additional cost.
3.2.2. Attaching to T-bar support rods is not acceptable. Anchors for hangers must not be drilled into post-tensioned beams under any circumstances. Do not use Pneumatic hammers. All anchors must be drilled into the slab.
3.2.3. Do not 'fire spray' insulation during the installation of cable supports.

3.3. VELCRO STRAPS

- 3.3.1. Ensure Velcro straps is used to neatly dress cables; Ensure they are placed at a maximum of 1219 mm (48") intervals for horizontal distribution (centre points between cable supports).
3.3.2. Velcro straps also used to dress cables into racks/cabinets. Maximum spacing of Velcro for cables into or along vertical cable managers no more than 152 mm (6"), this includes cabling dropped from the ladder tray or ceiling above.

3.4. CABLE DISTRIBUTION

- 3.4.1. The minimum conduit bend radius is as per the manufacturer's recommendations.
3.4.2. Make cable pulls continuous and steady between pull points. Do not interrupt the pull unless necessitated by excessive tension on the cable.
3.4.3. Protect exposed cable ends from moisture ingress.

3.5. DUCT AND CONDUIT

- 3.5.1. Clean out each section of duct or conduit by pulling a steel wire brush and mandrel of the correct size through the duct or conduit before pulling cables. Bush, ream and remove any sharp projections on all conduits prior to installation of communications cables. When cleaning ducts, if obstructions are encountered which cannot be removed, advise the Electronic Safety and Security Engineer's Representative of the problems encountered.

- 3.5.2. Apply manufacturer's specified lubricant to cables to reduce friction between the cable and the conduit. Cable grip attached to the sheath and its strength members so that no direct force is applied to the conductors/fibres. The cable grip has a ball bearing swivel to prevent the cable from twisting during pulling.

END OF SECTION

28 05 53.00 Identification for Electronic Safety and Security

1. General

1.1. WORK INCLUDED

- 1.1.1. Provide A Class 3 system as per the latest version of the ANSI/TIA/EIA 606 Standards.
- 1.1.2. All elements of the Electronic Safety and Security Systems is labeled with unique identifiers.
- 1.1.3. Where labeling schemes are not provided co-develop a labeling scheme with the Owner and the Electronic Safety and Security Engineer's Representative before the installation of any permanent labels on the Electronic Safety and Security Systems components.
- 1.1.4. Labeling schemes are confirmed with the Electronic Safety and Security Engineer's Representative before installation.

2. Products

2.1. LABELS

- 2.1.1. Ensure all cable and equipment labels meet the legibility, defacement, and adhesion requirements specified in ANSI/UL 969. In addition, the labels are required to meet the general exposure requirements in ANSI/UL 969 for indoor and outdoor use.
- 2.1.2. When wrapped around a cable ensure Cable labels are of self-laminating vinyl construction with a white printing area and a clear tail that self-laminates the printed area. The clear area should be of sufficient length to wrap around the cable at least one and one-half times. The width is required to be sufficient to accommodate the appropriate label designation.
- 2.1.3. Provide vinyl substrate with a white printing area and black print. If cable jacket or equipment is white, provide cable label with printing area that is any other colour than white, preferably orange or yellow – so that the labels are easily distinguishable.
- 2.1.4. Ensure Labels are flexible vinyl or other substrates to apply easily and flex as cables are bent.
- 2.1.5. Ensure Labels use aggressive adhesives that stay attached even to the most difficult to adhere to jacketing.
- 2.1.6. Labels should be resistant to the environmental conditions at the point of installation (such as moisture, heat, or ultraviolet light) and should have a design life equal to or greater than that of the labeled component.
- 2.1.7. Ensure all labels are mechanically printed using a laser printer. Hand-written labels are not permitted.
- 2.1.8. All backbone and horizontal cables including patch cord labels are printed in 10 point Arial Narrow, black, bold font.
- 2.1.9. Ensure all equipment labels are printed in 14 point Arial Narrow, black, bold font.
- 2.1.10. Ensure all Hub, Main Cabinets, and controlling device enclosure labels are black lamacoid plates with white 60 point Arial Narrow, engraved upper case letters enclosed by a white border on black background.

3. Execution

3.1. LABELLING

- 3.1.1. Submit sample labels to Communications Consultant for approval before procurement and installation.
- 3.1.2. Provide all labels as indicated in this document and contract drawings.
- 3.1.3. Provide all labels for all cables and all active and passive devices, conduits, and pull boxes.
- 3.1.4. Label all ends of conduits including ends of conduits that terminate in pull boxes. Ensure all the label is installed within 304mm (12") of each conduit end. Label designations for conduit and pull boxes is confirmed with the consultant before procurements and installation. Allow for adding label designations (soft) for conduits and pull boxes to soft cabling schedules.
- 3.1.5. Ensure all Labels are located on cables and equipment as indicated in this document and on contract drawings.
- 3.1.6. Labels should be visible during the installation and normal maintenance of the infrastructure.
- 3.1.7. Ensure all Labels are affixed to the front and rear of equipment where required and 150 mm (6") from the end of all backbone and horizontal cables.
- 3.1.8. Labels are affixed 75 mm (3") from the end of all patch cords.
- 3.1.9. Labels should be attached at both ends of all cables (within 75 mm (3") of the end).
- 3.1.10. All temporary labels removed from cables and equipment before commissioning.
- 3.1.11. Ensure all labels are visible.
- 3.1.12. Ensure all active and passive equipment are labeled.

END OF SECTION

28 08 00.00 Commissioning of Electronic Safety and Security

1. General

1.1. NOT USED

2. Products

2.1. TEST EQUIPMENT

2.1.1. Provide portable two-way radios and or other communication devices.

2.2. PROPRIETARY TEST EQUIPMENT

2.2.1. Provide all proprietary test equipment that is required to facilitate testing and commissioning of the Electronic Safety Security System. All proprietary test equipment become the property of the Owner upon completion of the commissioning.

2.2.2. Obtain and review design documents for overall design intent and the overall required systems configurations.

2.2.3. Obtain and review shop drawings and submittals for installation criteria and the required construction details, as they support and further define the system's features.

2.2.4. Make general reviews at the job site and review the following for configuration:

- .1 Quality of construction
- .2 Adherence to design requirements
- .3 Conformance with shop drawings and submittal information.

3. Execution

3.1. COMMISSIONING PROCESS

- .1 Execute the following:
 - .1 Identify all systems, equipment, components, and functions to be commissioned
 - .2 Develop itemized test procedures including itemized functional test forms and device test checklists
 - .3 Review commissioning plan and process with the Electronic Safety and Security Engineer's Representative
 - .4 Perform pre-startup tests
 - .5 Perform device tests
 - .6 Perform functional tests
 - .7 Perform system integration functional tests
 - .8 Perform retests as necessary
 - .9 Turnover

3.2. COMMISSIONING

- .1 Identify all components, functions, and systems are commissioned.
- .2 Develop device checklists, functional test forms, and system integration test forms that are executed.
 - .1 Device Checklists
 - .1 Each device checklist includes but not limited to:
 - .1 Unique identifier of each device and component of the respective system
 - .2 Location of device
 - .3 Name of commissioning agent
 - .4 Name of witness
 - .5 Date of commissioning
 - .6 For each device; all functions and performance requirements indicated in the relative system specifications sections of this document, all function and performance requirements indicated on all associated drawings, all industry-standard tests, all manufacturer-recommended tests, all test that are required to confirm that the respective device is in proper working order.
 - .7 Confirmation of device tests performed
 - .8 Confirmation of tests passed or failed and related comment
 - .2 Functional Test Forms
 - .1 Each functional test form includes but not limited to:
 - .1 Identification of system under test
 - .2 Location of system
 - .3 Name of commissioning agent
 - .4 Name of witness
 - .5 Date of commissioning
 - .6 For each system; all function and performance requirements indicated in the relative system specifications sections of this document, all functions indicated on all associated drawings, all industry-standard functional tests, all manufacturer-recommended functional tests, and all functional tests that are required to confirm that the respective system is in proper working order.
 - .7 Confirmation of functional tests performed
 - .8 Confirmation of tests passed or failed and related comment
 - .9 For each video surveillance camera; include a video surveillance camera "Field of View Sample Snapshot" area in addition to all the above noted functional tests
 - .3 Systems Integration Functional Test Forms
 - .1 Each system integration test form includes but not limited to:
 - .1 Identification of systems under test
 - .2 Location of systems
 - .3 Name of commissioning agent

- .4 Name of witness
- .5 Date of commissioning
- .6 All integrated functions and performance requirements that are indicated in the electronic safety and security system integration specifications section of this document, all integrated functions indicated on all associated drawings, all industry-standard integration functional tests, all manufacturer-recommended integrated functional tests, and all integrated functional tests that are required to confirm that the respective systems are integrated and are in proper working order.
- .7 Confirmation of integrated functional tests performed
- .8 Confirmation of tests passed or failed and related comment
- .3 Forward the device checklists, functional test forms, and systems integration test forms to the Electronic Safety and Security Engineer's Representative for review and approval before commencing commissioning.
- .4 Pre-Start-up Test
 - .1 Perform pre-startup tests to verify that the devices and systems that are to be commissioned are powered, calibrated, operational, and ready for device and functional testing.
- .5 Perform Device Tests
 - .1 Perform device tests for all devices following the device checklists.
- .6 Perform Functional Tests
 - .1 Perform functional tests for all devices and systems following the functional test forms.
- .7 Perform System Integration Tests
 - .1 Perform system integration functional tests for all devices and systems following the system integration functional test forms.
- .8 Perform Retests as Necessary
 - .1 For all failed tests, make all necessary repairs and perform retests. Failure of the integrated test may require the retest of one or more individual tests. Conduct repairs and retests until all tests are passed.
- .9 Turnover
 - .1 Prepare a comprehensive commissioning report that includes but not limited to completed device checklists, completed functional test forms, completed systems integration functional test forms with measured data. The commissioning report is submitted along with system operation and maintenance manuals for review and approval by the Electronic Safety and Security Engineer's Representative.
- 3.3. ACCEPTANCE CRITERIA
 - 3.3.1. To be determined by the Electronic Safety and Security Engineer's Representative.
- 3.4. ACCEPTANCE PROCEDURES
 - 3.4.1. To be determined by the Electronic Safety and Security Engineer's Representative

- 3.4.2. To ensure the Owner and all contracting parties agree, a formal acceptance procedure has been established for the security sub-system of this Division. The acceptance is based on the successful completion of the testing requirements and therefore not open for punch list items. Final acceptance of the commissioning is when all tests are completed and the results of the tests are reviewed and accepted by Electronic Safety and Security Engineer's Representative.

END OF SECTION

28 08 00.00 Access Control

1. General

1.1. PURPOSE

- 1.1.1. The building's and facility's Access Control System's primary function is to protect the assets. The contents of this document are critical and are considered confidential. Ensure this information is not disclosed to anyone other than authorized personnel.

1.2. SCOPE OF WORK

- 1.2.1. The work covered by this section includes the furnishing, installation, and activation of all equipment & materials associated with the complete Access Control System as shown and as specified herein. This work may include, integration with the associated subsystems and components listed in these sections.
- 1.2.2. Ensure new products integrate with the existing system.

1.3. CONTROLLER SYSTEM FUNCTION AND PERFORMANCE REQUIREMENTS

- 1.3.1. The Access Control System is as described in this specification and illustrated on the drawings.

- .1 Access control software
- .2 Access control server
- .3 Personal computers
- .4 Detecting and controlling devices
- .5 Credential Readers
- .6 Credentials
- .7 Wired Electrified Door Locks
- .8 Power supplies

- 1.3.2. Ensure system have the following minimum functions:

- .1 Regulate and monitor access at system-controlled doors.
- .2 Control access to elevator floors and monitor elevator floor button activity.
- .3 Monitor and control access to parking lots/parking garages.
- .4 Monitor connected detectors (supervised and auxiliary inputs) with the ability to manually or automatically arm and disarm them.
- .5 Control event initiated devices connected to system outputs, such as alarms or video recorders, with the ability to automatically or manually arm or disarm them.
- .6 Report alarm conditions.
- .7 Distribute an annunciated alarm condition via an email notification off-site.
- .8 Establish a hierarchy of alarm types to prioritize handling alarm conditions.
- .9 Maintain a comprehensive database recording all site activity.
- .10 Integrate with the new Video Surveillance system.

- .11 Operate fully integrated photo badge and verification applications allowing for complete ID badging operation.
 - .12 Include fully integrated active mapping functions.
 - .13 Include fully integrated visitor management functions.
 - .14 Include fully integrated guard tour functions.
 - .15 Integrate with intrusion detection systems controllers.
 - .16 Facilitate full functions via remote access. Ensure Remote access is via the Internet or a corporate intranet with a Web application.
- 1.3.3. Building Integration
- .1 Ensure the system is able to integrate multiple buildings within one collective access control/alarm monitoring entity whether the buildings are in relative proximity or at distant locations. The access control system's design shall further allow expansion or modification within existing buildings or the integration of buildings at any time.
 - .2 Ensure the system is structured to provide a continually expandable growth path from the functions and features specified within this document without the necessity of exchanging previously installed controllers or software.
- 1.3.4. Communication
- .1 The software and devices communicate using one or a combination of the following connection modes:
 - .1 Network (TCP/IP)
 - .2 Wireless networks
 - .3 Internet
 - .4 Serial (RS-232)
 - .5 Serial (RS-485)
 - .6 Wiegand and OSDP
- 1.3.5. Multiple System Users
- .1 The system supports multiple system user central management station with access to the system database. The number of concurrent users is only limited by the software licensing agreement.
 - .2 Ensure the software provide selectable controls to govern individual user activity with log-on accounts and passwords. System user activity is recorded to the database and accessible for operator audit and review.
 - .3 Ensure the system software provide an application that allows multiple users remote connectivity via a corporate intranet or the Internet to input and manage selective system functions.
 - .4 Partitioning system to be divided into multiple data partitions. Partition administrators can fully add personnel cardholders and produce ID badges on their partition but are prevented from seeing the data of other partitions that reside on the same server.
- 1.3.6. Cardholder Access
- .1 Ensure the Cardholder Access is governed by a controlled entry point (doors) using an assigned credential such as a card, fob, PIN, biometric or mobile that is presented to a sensing device referred to as a card reader.
 - .2 Ensure at least one credential is supplied for each individual who requires access through the controlled doors.

- .3 Ensure the system supports the following reader formats:
 - .1 Proximity (13.56 MHz and 125 kHz)
 - .2 Mifare Contactless Smart Card
 - .3 Latest FIPS and TWIC applicable standards
 - .4 Large Card Format (up to 75 bits)
 - .5 HID Corporate 1000
 - .6 Radiofrequency transmitter/HID proximity combination
 - .7 Biometrics
 - .8 Contactless Smart Card & iClass
 - .9 Personal Identification Number (PIN) only
 - .10 Barcode
 - .11 Bluetooth
 - .4 Each credential is internally encoded with an individual number. Ensure the system provides the means to enter these numbers into a database for transmission to each controller.
 - .5 The reader scans the internal number encoded in each credential and transmit this information to the controller.
 - .6 The controller processes the credential data and unlock the appropriately controlled door only if the credential is determined to be valid for access through that door.
 - .7
 - .8 An access request at a reader is determined based on the following conditions. Should any of the conditions be false, access would be denied. This results in an 'Access Denied' event recorded in the database.
 - .1 Is the card valid for this day?
 - .2 Is the card valid for this time?
 - .3 Is today a holiday? If yes, is the card valid for this holiday?
 - .4 Does the PIN match the card presented?
 - .5 Is the card valid for this site?
 - .6 Is the card valid for this door?
 - .9 Doors are unlocked for valid cardholders requesting entry within one second following the reader scan regardless of all other system activity.
- 1.3.7. Door Identification and Control
- .1 Ensure system provide the means to identify each portal or door that is controlled by a controller with a unique alpha description and provide the following controls or functions:
 - .1 User-defined door relay unlocks time of 2 to 99 seconds, adjustable in 1-second increments.
 - .2 The user-defined door held open time of 2 to 99 seconds, adjustable in 1-second increments.
 - .3 Controllers automatically re-lock the controlled portal when the door is sensed as closed or when the door relay unlock time expires.

- .4 Provide a handicap accessibility feature such that an access control relay can be connected to a door operator with separate door time settings.
 - .5 Provide a pre-alert that advises when a door remains open at the half interval of the door held open time.
 - .6 Ensure each controller provide a dedicated request to exit input for each door (i.e. motion request to exit device, an exit button, etc.).
 - .7 The above access modes may be set to time zones with the ability to automatically institute a change in the access mode at any time within a 24 hour clock to satisfy security requirements.
 - .8 Monitor the status of all doors controlled by controllers with the status stated in one of the following conditions:
 - .1 Locked
 - .2 Unlocked
 - .9 Provide a manual override to lock or unlock doors controlled by the access control units.
 - .10 Provide a programmable facility to automatically unlock and relock specified doors during an assigned time zone to allow access without the use of a token or card.
 - .11 Provide programing to prevent assigned doors programmed for auto-unlock from unlocking at the start of a designated time zone until a valid card is first presented by an authorized cardholder.
 - .2 Anti-Pass Back
 - .1 Ensure system allow doors to be anti-pass back enabled. Anti-pass back is restricted to monitoring and enforcing IN/OUT conditions at doors connected to the same access control unit.
 - .2 A manual override is incorporated into the 'anti-pass back' function.
 - .3 Ensure the system has multiple modes of local anti-pass back:
 - .1 Hard mode – designated cardholders are denied access on violating anti-pass back enforcement
 - .2 Soft mode – designated cardholders are allowed access but an anti-pass back violation is reported
 - .3 Timed mode – designated cardholders are denied access on violating anti-pass back enforcement except anti-pass back enforcement is based on a time interval (can be employed on a single reader)
 - .4 Executive mode – excludes designated cardholders from anti-pass back enforcement
- 1.3.8. Alarm Monitoring Functions
- .1 Ensure the system provide forced entry detection at secure door locations. A forced entry is generated immediately whenever the door is opened without authorization. Authorization is determined by a credential or request to exit transaction at the door or by command from the system.
 - .2 Ensure the system provide door held open detection at controller-controlled doors. A door held open event is generated immediately whenever the door is held open longer than its specified time limit.

- .3 Ensure the system features the provision to monitor auxiliary and supervised input points or detection zones. The system detects state changes between four distinct conditions for each of these points:
 - .1 Alarm
 - .2 Secure
 - .3 Trouble due to open circuit wiring
 - .4 Trouble due to short circuit wiring
 - .4 Ensure the system provides reader supervision to detect and report one of the following alarm conditions:
 - .1 Reader communication failure
 - .2 Reader tamper alarm
 - .5 When any change of state on an input point is detected, the systems is notified and generates a message stating the nature of the alarm, the location, and the time. The system records the alarm such that it can be later retrieved for an audit report.
- 1.3.9. Control Of Event Initiated Devices
- .1 Ensure the system have the ability to control event-initiated devices that respond to alarm events. Said devices may be armed or disarmed automatically by user-defined time zones or armed and disarmed manually by operator intervention.
 - .2 The condition for each alarm output is user-defined to include any of the following:
 - .1 Forced entry at a system controlled door
 - .2 Door held open time violation of a system controlled door
 - .3 Monitored alarm point detects a violation
 - .3 Ensure the system provide an alarm in the event a controller is tampered with.
- 1.3.10. Communication Failures
- .1 The system notifies the central management station of any communication failures with controllers or the communication application.
- 1.3.11. Ensure the system software provides full integration of all system components for overall access control management. The system software is regulated by individuals deemed as system operators. The system software includes the following specifications:
- .1 User Interface
 - .1 Ensure the main screen has pull down menus as well as quick buttons for direct access to frequently used functions.
 - .2 Ensure the software provides multiple language interfaces:
 - .1 English
 - .2 French
 - .3 Ensure the software is designed to allow each operator to select a language of his or her preference and at any time change languages without having to exit and re-start the software. The software further supports concurrent operators to work with different interface languages simultaneously and have access to context-sensitive help in the operator's choice of language.
 - .4 The software employs keyboard shortcuts for rapid access to certain functions.
 - .5 Ensure the operator is able to run the system software in a minimized state and still receive notification of alarm events.

- .6 Ensure the system interface provides formatted forms for facility management. These forms provide the user with the ability to add, edit, delete, or view site-specific information including instructions about alarms and emergencies.
- .7 The system provides the operator with the ability to add, edit or view the following functions:
 - .1 site information and access control units
 - .2 Elevator floor control
 - .3 door and elevator group access levels and associated time zones for each door and elevator floor
 - .4 cardholder records
 - .5 administrator/operator records
 - .6 readers/doors in the system
 - .7 elevator information
 - .8 time zones, schedules, holiday types, and holiday dates
 - .9 alarm response instructions and contacts
 - .10 manual overrides & system utilities
- .8 Ensure the system further provide the operator with the facility to define, view, and print summaries based on system-wide activity recorded by the database.
- .2 System Software Requirements
 - .1 Ensure the system is based on independent, intelligent devices that are interconnected and communicate to rack-mount Access Control System Servers.
 - .2 Provide all servers in all configurations as required for a complete and operational access control system.
- .3 Software Architecture
 - .1 Ensure the system software is designed so that it can be installed on a single PC or on multiple PCs and in both circumstances operate on a LAN/WAN (TCP/IP) from any communication node on the network.
 - .2 Acceptable database engines
 - .1 Oracle RDBMS, IBM DB2, Microsoft SQL Server, MySQL, and PostgreSQL.
- .4 Owner Software
 - .1 Event processing, data entry, system management functions, and auditing system activity is performed from a PC.
 - .2 The system supports multiple concurrent Owner-operators commensurate with the license agreement.
 - .3 The system software program and monitor remote site systems simultaneously.
 - .4 The system software support digital signature capture devices with integrated software.
 - .5 The system software provides the means of streaming site activity data to a serially connected device such as a pager.
 - .6 Alarm Annunciation And Processing
 - .1 System occurrences deemed as violations articulated as alarm events at the computer.

- .2 Ensure the system software allow assigning user-defined names for any reader port or input point to distinguish its location for the benefit of the operator.
- .3 The system further provides the following alarm notification/processing:
 - .1 Display the alarm in an alarm events window that cites crucial alarm information for expedient alarm handling.
 - .2 An alarm notification pop-up window come to the foreground so long as the access control Owner program is running.
 - .3 An audible warning sounds
 - .4 Ensure the system provide a designated form with specific alarm event information and instructions accessible to the operator. The information shown include:
 - (i) Alarm time
 - (ii) Alarm type
 - (iii) User-defined description
 - (iv) Location
 - (v) Alarm response instructions
 - (vi) Alarm contacts
 - (vii) Alarm response comments
 - .5 It is possible for the operator to acknowledge an alarm clearing it from the alarm events window or defer an alarm for further investigation.
 - .6 The operator is provided with the means to cite and save commentary on the disposition of an alarm event.
 - .7 Ensure the systems is integrated with the Video Surveillance system and provide all operators with the means to view is located still images captured by the associated cameras during the alarm event.
 - .8 As an additional aid to the alarm event, ensure the system provide all operators with the option to open a floor map to pin-point the location of the door or device that tripped the alarm. Complete floor maps/plans of all floors where access control system device/s are located is provided, imported, and integrated with the access control system to provide such functions.
 - .9 Ensure the system allows the operator to examine information for all alarms currently waiting for processing one at a time without acknowledging them and/or clear all alarms in the system.
 - .10 Ensure the system database logs each occurrence of an alarm event.
 - .11 The system operator is furnished with the means to view current or pending alarms or search for alarms by device type, by a specific controller, by alarm type, by site name, or by a date range.
 - .12 The system incorporates the ability to email an alarm or critical message to a device that has an Internet email address.

- .13 Ensure the system provides the means to establish a hierarchy of alarm priority levels to assist operators in determining an alarm's degree of importance. The system allows user-defined properties to be assigned to each alarm priority:
 - (i) Each alarm priority can be assigned to an access control unit, a door, an auxiliary input, a supervised input, or an optional input device with each device assigned to a specific alarm type or group of alarm types.
 - (ii) Each alarm priority can be assigned a unique description with customized display characteristics.
 - (iii) Each alarm priority can be assigned to a system time zone to regulate when the alarm priority is in effect. When the time zone is not in effect, the alarm is still reported but without its assigned properties.
 - (iv) Each alarm priority can be routed to specific logged-on system operators at specific computers.
 - (v) Each alarm priority can be assigned a sound (WAV) file to audibly annunciate the alarm priority to assist the operator in distinguishing the level of alarm importance
- .14 In the event of AC power failure to the access control units, ensure the system software have the means to report the AC power failure as an alarm with user-selectable time duration before the alarm is tripped.
- .15 Where keypads are installed, the system provides a duress alarm type. A distressed cardholder would press the designated duress key then enter the PIN code. The system would allow access and annunciate a duress alarm for an expedient response to the situation.
- .7 Building Emergencies/Evacuations/Lockdowns
 - .1 Ensure the system provides the means to automatically generate a printed card IN/OUT status report which can be used in emergencies or building evacuations to determine who is in and out of the building.
 - .1 The card IN/OUT status report printout can be set to specified timed intervals for continuous updating until the emergency or situation is resolved.
 - .2 The card IN/OUT status report can be emailed for remote location notification.
 - .2 Ensure system provide an optional standalone executable lockdown application designed to turn off one or multiple time zones to affect a lockdown.
 - .1 The lockdown is designed to be triggered on a transaction-type event such as a card presentation at a reader for rapid reaction to an emergency.
 - .2 The system is able to lock down all doors regulated by the time zone that has been turned off for maximum system-wide control.
- .8 Cardholders

- .1 Ensure the system software provides system-defined fields and user-defined fields to identify each cardholder.
 - .2 Ensure the system also provide the ability to insert a digital photograph on each cardholder record (optional). The photographs may be inserted on ID cards or displayed while observing online transactions to enhance security protocols.
 - .3 Ensure the system stores cardholder new images in the database.
 - .4 Ensure the system provide the ability to designate cardholders with temporary status and restrict the card to a defined date range and/or a maximum number of uses. After the date range or when the number of uses reaches zero, the system renders the card inactive and deny further entry.
 - .5 Ensure an operator is able to view from each cardholder record the last 25 transactions over the previous 7 days for auditing, investigating activity, or locating a cardholder's whereabouts.
 - .6 The system furnishes a mechanism to load blocks of numerically sequenced cards with the same facility code for expedient card loading.
 - .7 Where multiple sites exist, ensure the system provide the means to quickly copy cardholder records to alternative sites. Each cardholder who requires access to multiple sites require only one card to access all authorized sites.
 - .8 In the event, a card is lost or stolen or upon employment termination, ensure the system allows a card to be canceled and rendered invalid within seconds.
 - .9 As an alternative to permanently deleting a card, the system allows a cardholder record to be designated as 'Archived'. While the archived status is in effect, the record is maintained in the database but the card is invalid and denied entry to all previously authorized access points. The archived status remain in effect until it is re-activated by an operator.
 - .10 To locate and review cardholder records, the system provides extensive search functions that allow broad latitude of cardholder search criteria to retrieve one or multiple cardholder records. The system also includes a search criterion entitled 'Not Used Since' that lists inactive cards based on a defined date for maintaining up-to-date records.
 - .11 Ensure system exports cardholder records in Acrobat® PDF format for the benefit of non-system users.
 - .12 Ensure system also provides a time-saving mechanism to import and export cardholder records as CSV files with other external databases. This allows transferring cardholder records to and from the access control database reducing data entry.
 - .13 Ensure system provide a facility to view an access level summary for individual cardholders to determine which system-regulated doors and elevator floors are and are not accessible to the cardholder.
- .9 Time Zones And Schedules
- .1 Ensure the system provides minimum 256 time zones (254 are user-definable) and minimum 512 schedules for door and elevator control and input, and output points.

- .2 Each time zone and schedule are configurable within a minimum seven (7) day week.
- .3 Ensure that the system provides a minimum three (3) holiday schedules which can be used as overrides to regular time zones and schedules for statutory holidays, special occasions, plant shutdowns etc.
- .4 Ensure the system supports a minimum of sixty-four (64) holiday dates that the three (3) holiday schedules can be assigned to. When a holiday date is in effect, the assigned holiday type schedule overrides the time zone for that date. The system further provides a facility to specify recurring holidays eliminating the need of resetting those holidays each year.
- .5 If holidays have been specified, the system list all holiday dates and types.
- .6 Ensure the system automatically invoke a holiday schedule when the system clock matches any date defined as a holiday. A holiday schedule overrides all other time zones and schedules. Access is predicated on the times and authorizations of the holiday schedule for the stated holiday date. At the start of the next non-holiday calendar date, the system invokes the regular time zone settings and access conditions.
- .10 Door Group Access Levels
 - .1 Ensure the system allows creating minimum 511 door groups of which each cardholder may be assigned to minimum 2 door groups
 - .2 The system as a means for providing greater security and control segregate door into separate entities with independent time zones and access levels.
 - .3 Ensure the system provides the following three access levels for door groups and elevator groups:
 - .1 24-hour access
 - .2 No access
 - .3 Access based on a time zone
- .11 System Operators
 - .1 Ensure the system provides the means to maintain a secure administrative environment. Only operators given an administrator account with a unique User ID and Password are permitted access to the system software. Unauthorized individuals are denied access to the system software.
 - .2 Ensure the system provides a means of setting discretionary operator functionality for each user account.
 - .3 Ensure the system allow each operator individualized access for adding, editing, deleting, and viewing database information, as well as interrogating and issuing commands to the controllers depending on the functions enabled in the operator's account.
 - .4 The system supports an unlimited number of system operator accounts. Ensure Passwords are not be displayed or printed by the system at any time during usage. It is possible to change passwords at any time.
 - .5 Ensure the system provide the means of tracking operator activity generate detailed summaries of activities.
- .12 Manual Overrides

- .1 Ensure the system furnish an operator with manual control of doors from an Owner computer as detailed below:
 - .1 Unlock a door and leave it unlocked
 - .2 Unlock a door momentarily, such that it automatically re-locks after the normal door relay unlock interval
 - .3 Lock a door
 - .4 Unlock or lock all doors controlled by a selected controller
 - .5 Unlock or lock all doors for the currently logged on site
 - .6 Schedule a timed unlock period for a specified door
- .2 Ensure the system provide an operator with the ability to manually override elevator floor control by toggling individual or all floors to secured or unsecured. The system allows the operator to restore the elevator floors to their regulated state.
- .3 Ensure the system provide an operator with the means to manually arm or disarm auxiliary and supervised inputs and outputs. The system allows the operator to restore the inputs to their regulated state.
- .13 Other Control
 - .1 Ensure the system provide a function that allows a designated cardholder to independently invoke a change of state for specified doors and devices when a card is presented at a specified reader.
 - .2 Ensure the system is able to lock or unlock doors on an unscheduled basis, arm or disarm points connected to devices such as motion sensors, lockout other cardholders to prevent false alarms, implement a supervisory override to restrict access, or control lights, HVAC systems, etc.
 - .3 The system toggles a door's lock/unlock state or toggling a time zone's off/on state and provide the following multiple modes of operation:
 - .1 Door Toggle
 - .2 Time Zone Toggle with Cardholder Lockout
 - .3 Time Zone Toggle with Cardholder Lockout and Exit Delay
 - .4 Time Zone Toggle without Cardholder Lockout
- .14 Daylight Savings
 - .1 Ensure the system provides an interface that allows the operator to set daylight savings hours for multiple buildings with different time zones and or observing or not observing daylight savings hours. After operator input and controller uploading, ensure the system update all access control units with the time changes. The system is not be dependent on an adjustment of the computer's clock to affect the time changes.
- .15 Site Management Activity Reports
 - .1 Ensure the system furnish the operator with the function of transposing site activity recorded by the database into any of the following report types:
 - .1 Transaction Report
 - .2 System Log Entry Report
 - .3 Alarm Listings Report
 - .4 Cumulative Hours Report

- .5 Card In/Out Status Report
 - .6 Deleted Cardholder Reports
 - .2 Ensure the system furnish the operator with the ability to filter reports based on specifying relevant field criteria and Create custom reports without additional cost.
 - .3 In the case of Transaction Reports, the system allows an operator to automatically schedule the system software to self-generate a formatted report. The system further provides a mechanism to automatically send the report to a specified email address.
 - .4 To allow reports to be distributed to non-system users, the system software will the ability to save reports in Acrobat® PDF format and in some instances CSV format.
 - .5 Where a controlled enter/exit environment exists, ensure the system provides the means to generate a cumulative hours report (optional) specifying when cardholders entered and exited access points.
 - .6 Where a controlled enter/exit environment exists, ensure the system provide a cardholder status report as to whether the card is in or out.
 - .7 Ensure the system provide the operator with a report previewer to review the results of the specified report request.
- .16 System Settings Reports
- .1 Ensure the system furnish the operator with the function of generating system settings reports including the following summaries:
 - .1 Site Setup Report
 - .2 Reader Access Level Report
 - .3 Cardholder Report
 - .4 System Users Report
 - .2 To allow reports to be distributed to non-system users, the system software will have the ability to save reports in Acrobat® PDF format and in some instances CSV format.
 - .3 Ensure the system provides the operator with a report previewer to review the results of the specified report request.
- .17 Printing Reports And System Information
- .1 Ensure the system provides print functions on transaction reports and other system information.
 - .2 Ensure the system allows the operator to direct a print request to the printer interfaced with the operating system. The report is fully formatted complete with report name, headings, page numbers, time and date, and site name.
 - .3 The system is on monitor printer status. Ensure the operator is advised whenever the printer is not available.
- .18 On-Line Transactions
- .1 Ensure the system enables an operator to view site transactions as each event occurs for enhanced facility security. The operator is able to view up to 3 separate online transaction windows simultaneously.

- .2 The operator can use an array of filters to list only the desired transactions or transaction types on screen.
- .3 The system allows an operator to view transactions for remote sites in different time zones in real-time.
- .4 Ensure the system shows photos and details of cardholders enacting the transaction.
- .5 Ensure the online transaction window has a "card enrollment" function in which an operator has the convenience of enrolling an unregistered card that has been presented at a reader.
- .19 System Status
 - .1 Ensure the software provide the means to list all PCs and associated access control applications currently logged on the system.
- .5 Database Management
 - .1 Ensure the system record all operator input data, all operator tasks, all site(s) activity, and all alarm events to the database. Ensure the database is ODBC compliant.
 - .2 System-wide database information is stored on a hard drive within the host computer. The system database storage capacity is limited only by the hard disk capacity or the limitation of the server application.
 - .3 Ensure the system database information is distributed among all controllers as well as stored on the access control system server.
 - .4 The system advises the operator when the database has reached 75% of its maximum allowable size.
 - .5 The system has the provision to automatically upload to the controllers added, edited, or deleted database information that pertains to time zones, cardholders, operators, or access levels without operator intervention.
 - .6 The system interface advises the operator whenever the controllers require uploading other changes made to the database. This ensures all devices operate according to the most current information. The system performs database uploads to the controllers on demand.
 - .7 Ensure the system provide the facility to automatically backup the database on a user-defined schedule. During the backup of the database file, ensure there are no interruption to the system and the ongoing collection of data.
 - .8 Ensure the system provide the operator with the option to automatically purge old database backup files based on a "days lapsed" format. The system further provides the option of viewing in CSV format the average number of daily transactions for the specified purge-files date range.
 - .9 Database files can be backed up onto another medium such as a writable USB drives and CDs while the database events continue to be recorded without interruption to the collection of system activity.
 - .10 The contents of the database are available to operators for retrieving site information in user-defined reports.
 - .11 Ensure the system exports and import the cardholder segment of the database in CSV format. Ensure the system further provide the option to automatically schedule the software to import cardholder CSV files by time and day.
- .6 Database Disaster Recovery

- .1 Ensure the system include a disaster recovery utility as a means of recovering site data in the event that the database is lost because of file corruption, computer malfunction, or hard disk breakdown.
- .2 The disaster recovery utility download data stored in the access control units and retrieve crucial site information including all or partial cardholder names to the database in a quick and timely manner to re-establish full operation of the access control system.
- .3 Ensure the disaster recovery utility is able to recover data from all controllers whether they are located on one site or multiple sites.
- .7 Remote Internet/Intranet Access
 - .1 Ensure the system provide an Internet/Intranet Access application that allows remote connectivity for managing system functions.
 - .2 Ensure the Internet/Intranet application have user ID and password authentication for secure log-on.
 - .3 The Internet/Intranet application include the following functions:
 - .1 Add, edit, or delete cardholder records
 - .2 Show or modify door group and elevator group access levels
 - .3 Manually toggle elevator floor buttons to secure and unsecure
 - .4 Format and produce transaction reports
 - .5 View door status, lock, unlock, or pulse system controlled doors
 - .4 The Internet/Intranet is programmed with an automatic logout function. After a lapsed time of mouse or keystroke inactivity, the application automatically logs the user out to protect the site from potential unauthorized user activity.
- .8 Video Surveillance And Video Control System
 - .1 Ensure the system provides a Video Surveillance application module to integrate with the video surveillance system with the access control system. The system is not proprietary to the access control system.
 - .2 The operator is able to program cameras to activate on selected alarm events.
 - .3 Ensure the operator has the ability to view a live video feed with camera selection and view mode options or retrieve historical video from past alarm events.
 - .4 Ensure the operator have the option to open multiple Video Surveillance screens simultaneously for enhanced monitoring.
 - .5 Ensure system interface with compatible Digital Video Recorders (DVR), Network Video Recorders (NVR), IP addressable cameras, RS-485 and RS-232 platform multiplexers. DVRs and NVRs provide the ability to view the recorded images for an alarm event pinpointing the exact event that was recorded during the alarm.
- .9 Software Development Kit (SDK)
 - .1 Ensure the system interface with a software development kit allowing a third-party application to manipulate underlying access control software program functions as well as create customized integration and integration functions with all systems listed in the Electronic Safety and Security Systems Integration section.
- .10 Intrusion Controller Integration

- .1 The system provides intrusion controller integration software compatible with burglar alarm controllers which can monitor the current status of zones/partitions as well as other critical functions, such as battery status, controller AC status, and fire status.
- .2 The software allows an operator to manually arm or disarm individual partitions or configuring target readers for remote arming and disarming of partitions.
- .3 Ensure the system also provide a mechanism to insert icons representing alarm partitions on an "active map" for real-time monitoring with manual arming and disarming overrides.
- .11 Output Module
 - .1 Ensure the system provide an optional module that outputs data in a flat-file format (CSV) that can be integrated with 3rd party software.
- .12 ASCII Output
 - .1 Ensure the system provide a facility to output data serially in ASCII format.
- .13 On-Line Help, Manuals, And Setup Aids
 - .1 Ensure the system provide context-sensitive help and is presented in the same language as the user interface on the Owner module:
 - .1 English
 - .2 French
 - .2 The online help is context-sensitive whereby, when the operator presses a designated key, the relevant help screen opens.
 - .3 Ensure the system include an electronic copy of a software installation guide.
 - .4 The system's Owner application has a setup function that directs the operator through the process of setting up a site.
- 1.3.12. Provide (1) Server and four (4) Client Software licenses (2 to be deployed on-site and 2 for future Owner's use).
- 2. Products
 - 2.1. GENERAL
 - 2.1.1. Where product model is specified and are deemed discontinued by the product manufacturer, provide the latest manufacturer recommend product model at the time of installation in leu of the specified model.
 - 2.1.2. Where product performance specifications are provided, provide the latest manufacturer product model at the time of installation.
 - 2.1.3. All products and materials must be new and approved in the pre-installation submittals.
 - 2.1.4. Exterior devices are sealed and protected against weather conditions including heat, cold, moisture, dust, and sand.
 - 2.1.5. Commercial-grade, high quality, and rated for the environment in which it is being installed
 - 2.1.6. Compatible with the access control system.
 - 2.2. ACCESS CONTROL SOFTWARE
 - 2.2.1. Avigilon Access Control Manager Enterprise

- 2.2.2. Genetec Security Center Synergis Enterprise
- 2.2.3. Software House Ccure 9000 Enterprise
- 2.2.4. Kantech EntraPass Enterprise
- 2.2.5. Keyscan Aurora
- 2.2.6. ICT Protégé GX Enterprise

- 2.3. DOOR CONTROLLER
 - 2.3.1. Avigilon
 - .1 Mercury LP1502 PoE+ Edge-capable Intelligent Controller
 - .2 Mercury LP4502 Intelligent Controller w/ Extended Applications
 - .3 Mercury MR62e Reader Interface Module w/ PoE+
 - .4 Mercury MR52-S3 Reader interface panel
 - 2.3.2. Genetec
 - .1
 - .2 Mercury LP1502 PoE+ Edge-capable Intelligent Controller
 - .3 Mercury LP4502 Intelligent Controller w/ Extended Applications
 - .4 Mercury MR62e Reader Interface Module w/ PoE+
 - .5 Mercury MR52-S3 Reader interface panel
 - 2.3.3. Software House
 - .1 Software House iSTAR Edge 4 Reader Controller
 - .2 Software House iSTAR Ultra LT 16 Reader Controller (Rack Mount)
 - .3 Software House iSTAR Ultra SE 32 Reader Controller (Rack Mount)
 - 2.3.4. Kantech
 - .1 KT1
 - .2 KT-400 PCB complete with KT-CAB4000LDR enclosure
 - 2.3.5. Keyscan
 - .1 Keyscan 4-Reader Access Control Unit Part No: CA4500
 - .2 Keyscan 8-Reader Access Control Unit CA8500
 - 2.3.6. ICT Protégé
 - .1 ICT Protégé PRT-CTRL-DIN Rail System Controller
 - .2 ICT Protégé PRT-RDM2-DIN-485 The Protege 2 Door Reader Expander
 - .3 ICT Protégé PRT-HRDM2-DIN The Protege Half DIN Rail 2 Door Reader Expander

- 2.4. INPUT / OUTPUT CONTROLLER
 - 2.4.1. Avigilon
 - .1 Mercury MR16IN-S3 Multi-device interface panel
 - .2 Mercury MR16OUT-S3 Multi-device interface panel
 - 2.4.2. Genetec

- .1 Mercury MR16IN-S3 Multi-device interface panel
 - .2 Mercury MR16OUT-S3 Multi-device interface panel
- 2.4.3. Software House
 - .1 Software House I8 Input Module, I8-CSI Input Module, R8 Output Module
- 2.4.4. Kantech
 - .1 Kantech KT-MOD-IO16 complete with enclosure
- 2.4.5. Keyscan
 - .1 Keyscan I/O Board with Enclosure & Power Supply IOCB1616
 - .2 Keyscan 8 Relay Output Control Board OCB8
- 2.4.6. ICT Protégé
 - .1 ICT Protégé PRT-CTRL-DI N Rail System Controller
 - .2 ICT Protégé PRT-RDM2-DIN-485 The Protege 2 Door Reader Expander
 - .3 ICT Protégé PRT-HRDM2-DIN The Protege Half DIN Rail 2 Door Reader Expander
- 2.5. CREDENTIAL READERS
- 2.5.1. Minimum Features:
 - .1 Compatible with access control controller
 - .2 13.56 MHz Credential Compatibility: HID Seos, HID iClass SE, HID iClass, HID MIFARE Clasic, HID DESFire EV1
 - .3 125 kHz Credential Compatibility: FSK (HID, AWID, Wavelynx)
 - .4 MIFARE DESFire EV1 & EV2 Credential Compatibility
 - .5 Wiegand Communication Protocol
 - .6 OSDP Communication Protocol
 - .7 LED Colour While Idle: Red
 - .8 LED Colour on Credential Read: Flash Green
 - .9 Audio on Card Read: Enabled
 - .10 Wiegand Tamper Settings: Enabled
 - .11 OSDP Tamper: Enabled
- 2.5.2. Approved Manufacturers:
 - .1 HID
 - .1 HID® Signo™ Reader 20 or equivalent
 - .2 HID® Signo™ Reader 40 or equivalent
 - .3 HID® Signo™ Keypad Reader 20K or equivalent
 - .4 HID® Signo™ Keypad Reader 40K or equivalent
 - .2 Wavelynx
 - Wavelynx ETHOS™ ET-20 Wall Mount or equivalent
 - .1 Wavelynx ETHOS™ ET-10 Mullion Mount or equivalent
 - .2 Wavelynx ETHOS™ ET-25 Keypad Reader or equivalent

2.6. CREDENTIALS

2.6.1. Provide the following credentials:

Credential	Quantity
HID® iCLASS® 200x iCLASS® or equivalent	
HID® iCLASS® 205x iCLASS Key II or equivalent	
HID® iCLASS® 2080 Clamshell Card or equivalent	
HID® Proximity 1386 ISOProx® II Card or equivalent	
HID® Proximity 1346 ProxKey III or equivalent	
HID® Proximity 1326 ProxCARD II® Clamshell Card or equivalent	
Wavelynx MIFARE DESFire® EV2 Card, 4K (P/N 50H4) 8K (P/N 50H8) or equivalent	
Wavelynx MIFARE DESFire® EV2 Card, 4K (P/N 50H4) 8K (P/N 50H8) or equivalent	
Wavelynx Dual Frequency Proximity + MIFARE DESFire® EV2 Card, 4K (P/N 50D4) 8K (P/N 50D8) or equivalent	
Wavelynx MIFARE DESFire® EV2 Keyfob 8K (P/N 60H8) or equivalent	

2.7. PERIPHERAL DEVICES

2.7.1. Magnetic Contacts (Steel)

- .1 1" dia. contact for use in steel doors.
- .2 Flush or surface mount as required
- .3 Self-lock mounting
- .4 Rugged Construction

2.7.2. Magnetic Contacts (Wood)

- .1 3/8" dia. contact for use in wood doors.
- .2 Flush or surface mount as required
- .3 "Wings" protect contact reed from being crushed from swelling wood
- .4 Superior false alarm immunity

2.7.3. Magnetic Contacts (Overhead Door)s

- .1 Miniature and low-profile design
- .2 Stainless steel armored cable for added security and reliability
- .3 Aluminum bar stock to resist corrosion in harsh environments
- .4 Floor or track mount as required

- 2.7.4. Request to Exit Detector
 - .1 Tyco Model T.REX-XL2-NL or approved equivalent.
- 2.7.5. Remote Release Button:
 - .1 Potter Surface Mount HUB-M or approved equivalent.
- 2.8. POWER SUPPLY
- 2.8.1. Power supplies include all controller power supplies, all electrified lock power supplies, and all peripheral device power supplies.
- 2.8.2. Provide separate power supplies for controllers, provide separate power supplies for maglocks, provide separate power supplies for electrified locks separate from maglocks (e.g., electric strikes, electric latch retraction, electric mortise locks), and provide separate power supplies for peripheral devices.
- 2.8.3. Ensure all controller and peripheral device power supplies provide a backup battery to facilitate the complete and simultaneous full operation of all connected and powered devices for up to three (3) hours operation upon loss of AC power. The controller retains database information for up to seven days upon loss of power.
- 2.8.4. Ensure all electrified lock power supplies except maglocks power supplies provide a backup battery to facilitate the complete and simultaneous full operation of all connected and powered devices for up to one (1) hour operation upon loss of AC power.
- 2.8.5. Ensure all maglock lock power supplies have the capacity to add a backup battery to facilitate the complete and simultaneous full operation of all connected and powered devices for up to one (1) hour operation upon loss of AC power.
- 2.8.6. Agency Listings
 - .1 UL Listed for Access Control Systems (UL294),
 - .2 Power Supplies for use with Burglar-Alarm Systems (UL603),
 - .3 Hospital Signaling and Nurse Call Equipment (UL1069),
 - .4 Power Supplies for Fire Protective Signaling Systems (UL1481),
 - .5 CUL Listed - CSA Standard C22.2 No.205-M1983, Signal Equipment.
- 2.8.7. Features/Specifications:
 - .1 Voltage: output as required to facilitate complete system operation.
 - .2 Amperage: Rating as required to facilitate the complete and simultaneous operation of all associated powered devices.
 - .3 Class 2 Rated power limited outputs.
 - .4 PTC (Positive Temperature Coefficient) protected outputs.
 - .1 Each connected and powered device is connected to a separate PTC power supply output.
 - .5 Fuse rating as required or complete operation of each connected and powered device
 - .6 115VAC 60Hz, input.
 - .7 Filtered and electronically regulated outputs.
 - .8 Short circuit and thermal overload protection.
 - .9 Built-in charger for sealed lead acid or gel-type battery backup.
 - .10 Zero voltage drop upon transfer to battery backup.

- .11 AC input and DC output LED indicators.
- .12 AC fail supervision.
- .13 Low battery and battery presence supervision.
- .14 Fire alarm system interface.

2.9. ACCESS CONTROL CONTROLLER ENCLOSURES

- 2.9.1. Provide access control controller enclosures to house and protect all controllers.
- 2.9.2. Ensure all access control controller enclosures are a single key locking metal box.
- 2.9.3. Size as required to house and protect all controllers.
- 2.9.4. Equipped with door tamper switch. Connect each door tamper switch to the access control system.
- 2.9.5. Equipped all enclosure doors with door tamper switch. Connect each door tamper switch to the intrusion detection system.
- 2.9.6. Ensure the quantity and size of access control controller enclosures does not exceed the real estate provided for mounting access control controller enclosures. Refer to contract drawings and coordinate as such.

2.10. ELECTRIFIED LOCKS

- 2.10.1. All electrified locks are provided by others.
- 2.10.2. Electrified locks include electric strikes, electric mortise locks, electric latch retraction, maglocks all electrified locks noted on project door hardware schedule and or architectural drawings and schedules.
- 2.10.3. Provide a separate power supply for electrified locking devices to facilitate the complete operation of all electrified locks.

3. Execution

3.1. COORDINATION

- 3.1.1. The ESSC is responsible for the systems specified in this Section, including coordination with related trades.
- 3.1.2. Engage a factory-authorized service representative to supervise and assist with startup service. Complete installation and startup checks in accordance with manufacturer's written instructions.
- 3.1.3. Ensure the ESSC coordinate all work and submittal details with the electronic door hardware supplier to ensure proper sizing of control equipment and is responsible for proper sizing of interface equipment (i.e., relays, contact ratings, etc.) to eliminate interface problems.
- 3.1.4. Provide the following related work:
 - .1 Coordination of all work related to the door hardware contractor, all electrified door hardware, and electrified locks.
 - .2 Provide all interface, wiring, and connections to all electrified door hardware and electrified locks as required to facilitate a complete and operational electronic access control system.

- .3 Related Electrical Works
- .4 Related Control Work and/or annunciation
- .5 All 120 Volt wiring and connections from a power source to terminal strips in electronic low-voltage controllers, power supplies, and devices.
- .6 Provide cable troughs, raceway, conduits, including all back boxes and pull strings and device-specific and or proprietary and or special back boxes.

3.2. CONTROLLERS AND PERIPHERAL DEVICES

- 3.2.1. Update all firmware and or reinstall the latest version of firmware on all controllers, credential readers, and all active devices.
- 3.2.2. Use tamper-proof security screws to secure credential readers.
- 3.2.3. Enable and connect tamper alarms for credential readers, controllers and all supervised active and passive devices.
- 3.2.4. Provide and install access control controllers/enclosures as required to house and protect all controllers.
- 3.2.5. Ensure all controllers and peripheral devices are installed and configured following the manufacturer's installation instructions and recommendations, as per the Owner's requirements and as per contract drawings and specifications.
- 3.2.6. Coordinate exact mounting locations of all controllers on-site with the Security Engineer's Representative and Owner.
- 3.2.7. Provide all peripheral devices where indicated on contract drawings and documents.
- 3.2.8. Refer to Architectural Door and Door Hardware Schedules and ensure that each peripheral device is coordinated with its respective door and door hardware.
- 3.2.9. Ensure peripheral devices are compatible with the access control system.
- 3.2.10. Submit shop drawings of all devices to the Security Engineer's Representative for approval before procurement and installation.
- 3.2.11. Allow for "needs assessment sessions" with the Owner to determine the exact mode/s of operation of each peripheral device.
- 3.2.12. Allow for configuration of the system and each peripheral device and each controller to suit the Owner's requirements.
- 3.2.13. Configure each motion request to exit the device to shunt door contact (magnetic contact) and allow free egress without alarms. Ensure motion request to exit the devices do not release respective electrified lock/s upon activation of said motion request to exit the device.
- 3.2.14. Configure the access control system so that presentation of a valid credential at a credential reader results in the release/opening of respective electrified lock/s.
- 3.2.15. Configure the access control system so that if a card reader is enabled and the respective electrified lock is locked by the system, activation of the respective automatic door operator actuators (wired and wireless buttons and motion/wave) on the **card reader** side of the respective door **does not** result in release/opening of respective electrified lock door.
- 3.2.16. Configure the access control system so that if a card reader is enabled and the respective electrified lock is locked by the system, activation of the respective automatic door operator actuators (wired and wireless buttons and motion/wave) on the **non-card reader** side of the respective **results** in release/opening of respective electrified lock and opening of the door.

- 3.2.17. Configure permissible door hold open timeframe on doors with auto door operators to 30 seconds. Configure permissible door hold open timeframe on doors without auto door operators to 15 seconds.
- 3.2.18. Allow for setup and configuration of card/credential holder database including adding each user to the database, enabling the access rights of each user and, programming of each user credential/s. Assume a total of 200 credential users.**POWER SUPPLY**
- 3.3.1. Provide power supplies as required for a fully functional access control system. Power supplies include all controller power supplies, all electric lock power supplies, and all peripheral device power supplies.
- 3.3.2. All power supplies are installed to the manufacturer's recommendations and as required to furnish a fully functional access control system.
- 3.3.3. Ensure power supplies are sized to facilitate the connection of each electrified lock and each powered device to separately fused power output.
- 3.4. **ELECTRIC LOCKS**
- 3.4.1. Electrified locks include:
 - .1 Electric strikes
 - .2 Magnetic locks/Maglocks
 - .3 Electric mortise locks
 - .4 Electric latch retraction
- 3.4.2. Make all wire connections to all electric locks as required for a complete access control system.
- 3.4.3. Provide wiring as required for the complete operation of all access control devices and systems.
- 3.4.4. Include all costs and work associated with acquiring permits for all magnetic locks.
- 3.5. **INSTALLATION**
- 3.5.1. Install all system components and appurtenances following the respective manufacturer's specifications, referenced practices, guidelines, and applicable codes. Furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signal, communications, and data transmission line grounding is installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.
- 3.5.2. Install the wiring system and integrate the system as indicated in this specification. All wiring is to be installed in a dedicated conduit throughout. Wiring is not pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring.
- 3.5.3. All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, are plenum rated where required by code.
- 3.5.4. All wiring conductors is individually numbered and each cable or wiring group being extended from a controller or cabinet to a building-mounted device is identified with the name and number of the particular device.
- 3.5.5. All exposed wiring inside and outside the control console, cabinets, boxes, and similar enclosures, are dressed down neatly and secured with wiring cleats or wire ties.

- 3.5.6. Ensure exposed metallic flexible conduit and armored cable is dressed down neatly and secured with low-profile, metal fasteners.
- 3.5.7. All cabinets, boxes, and similar enclosures containing security system components and/or cabling and which are easily accessible to employees or the public are provided with a lock. Boxes above ceiling level in occupied areas of the building is not considered to be accessible.
- 3.5.8. All junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public is covered with a suitable cover plate and secured with tamper-proof screws.
- 3.5.9. Ensure end-of-Line resistors is installed at the field device location and not at the controller location.
- 3.5.10. Riser diagrams are schematic and do not show every conduit, wire box, fitting, or other accessories. Provide such materials as necessary for a complete and functioning installation. Install following referenced codes and these specifications. Use weatherproof equipment or covers where installed in areas exposed to the weather.
- 3.5.11. Ensure equipment is mounted with sufficient clearance to meet all applicable codes and facilitate observation and testing. All equipment is securely fastened with appropriate fittings to ensure positive grounding and be free of ground loops.
- 3.5.12. Determine conductor requirements for each device following the Contract Documents and manufacturer requirements.
- 3.5.13. Install cable following Security System manufacturer requirements
- 3.5.14. Neatly route cables parallel or perpendicular to building lines.
- 3.5.15. Provide J hooks and other cable support systems (spaced at regular intervals) within accessible ceiling spaces. Fasten cables to the cable support systems and provide strain relief to protect cables and ensure compliance with required cable bends.
- 3.5.16. Keep cable not run in conduit a minimum of 18" from high voltage (120 VAC and above) circuits (e.g. light fixtures, wire run parallel with conduit, transformers, electric controllers, etc.).
- 3.5.17. Run cables at least six inches from the communications cable plant, intercom wires, input/output wires, and siren wires.
- 3.5.18. Route wire and cable as required preventing interference and signaling contamination of both Security System cable and cable associated with other systems. Coordinate the routing of wire and cable requiring isolation from power, radio frequency (RF), telephone, etc.
- 3.5.19. Provide sleeves and code-compliant fireproofing techniques for all penetrations of fire-rated partitions, masonry walls, and slabs, where the penetrations are made by or used for installation of Security Systems.
- 3.5.20. Separate high voltage (120 VAC and above) cables from low voltage cables within enclosures
- 3.5.21. Run wire and cable continuously from the device location to the final point of termination. No mid-run cable splices are allowed
- 3.5.22. Bundle and tie wire and cable with cable ties.
- 3.5.23. Cover exposed high voltage (120 VAC and above) power terminations within the controller, power distribution cabinets, and other security enclosures.
- 3.5.24. Labeled frames, doors, and enclosures
- 3.5.25. In no instance any UL labeled door, frame, or enclosure be drilled, cut, penetrated, or modified in any way.

- 3.5.26. Setup all data for access control software. Set up software and hardware and provide access to software to Owner.
- 3.5.27. Setup all controller features and access requirements.
- 3.5.28. Coordinate with the Owner and propose start and stop times for schedules, and configure entry schedules to entries.
- 3.5.29. Enable and configure alert settings.
- 3.5.30. Establish interlocks between alarms, intruder detection, and video surveillance integrations.
- 3.5.31. Develop all user-defined fields.
- 3.5.32. Create lockdown plans.
- 3.5.33. Coordinate with the Owner and establish badge layout options and design badges.

- 3.6. PROGRESS OBSERVATION
- 3.6.1. Security Engineer's Representative conduct progress observations during construction to verify construction progress and verify the construction schedule.
- 3.6.2. Security Engineer's Representative conduct the following minimum progress observations:
 - .1 Security Conduit Rough-in and Preliminary Wire and Cable Installation
 - .1 This observation intends to verify that adequate and proper conduit rough-in is installed, verify that wire and cable are being properly installed and labeled, and identify and resolve issues regarding conduit and wire and cable installation.
 - .2 Preliminary Wire Termination Progress
 - .1 This observation intends to verify that installations and equipment are following specifications and standards.
- 3.6.3. Observations occur upon initial installation of each type of equipment (i.e. Controllers, Card readers, alarm devices, junction boxes, etc.).
- 3.6.4. Observations must be complete before proceeding with the installation of remaining similar or like equipment.
- 3.6.5. Coordinate the appropriate timing of each observation with the general contractor, Security Engineer's Representative as required to meet intended goals.
- 3.6.6. The reviewers issue reports for each observation to summarize findings and document clarifications noted during the observation.

END OF SECTION

28 16 00.00 Intrusion Detection

1. General

1.1. GENERAL

- 1.1.1. The building's and facility's Intrusion Detection System's primary function is to protect the assets. The contents of this document are critical and are considered confidential. This information is not disclosed to anyone other than authorized personnel.
- 1.1.2. Where product model is specified and are deemed discontinued by the product manufacturer, provide the latest manufacturer recommend product model at the time of installation in leu of the specified model.
- 1.1.3. Where product performance specifications are provided, provide the latest manufacturer product model at the time of installation.
- 1.1.4. All products and materials must be new and approved in the pre-installation submittals.
- 1.1.5. Ensure exterior devices are sealed and protected against weather conditions including heat, cold, moisture, dust, and sand.
- 1.1.6. Commercial-grade, high quality, and rated for the environment in which it is being installed
- 1.1.7. Compatible with the intrusion detection system.

1.2. PURPOSE

- 1.2.1. The intrusion alarm system and accessories form part of the overall security strategy implemented and the system provides the real-time intrusion detection and data transmission.

1.3. SCOPE

- 1.3.1. The work covered by this section includes the furnishing, installation, and activation of all equipment & materials associated with complete intrusion detection systems as specified herein. This work may include, integration with the associated subsystems and components listed in these sections.
- 1.3.2. The requirements of the conditions of the Contract, Supplementary Conditions, and General requirements apply to the work specified in this section.

1.4. REFERENCES

- 1.4.1. Ensure Systems specified in this Section meet or exceed the requirements of the following:
 - .1 Underwriters Laboratories (UL/ULC):
 - .1 UL 365 – Police Station Connected Burglar Alarm Units and Systems
 - .2 UL 609 – Local Burglar Alarm Units and Systems
 - .3 UL 1076 – Proprietary Burglar Alarm Units and Systems
 - .4 UL 1610 – Central Station Burglar-Alarm Units
 - .5 ULC S301
 - .6 ULC-S302-14
 - .7 ULC-S304

.8 ULC Financial Burglary certificate

1.5. SYSTEM REQUIREMENT

1.5.1. General

- .1 Provide all intrusion detection system control panels and associated equipment, power supply, cabling, connectors, enclosures, and all other hardware and software to provide a fully operational system.
- .2 These "performance" specifications are to be translated into specific equipment and systems depicting proposed products.
- .3 Ensure the Intrusion Detection system is an interconnected group of components.
- .4 Ensure components are good quality commercial grade consisting of the following devices:
 - .1 Controllers and associated enclosures
 - .2 Communicators and associated enclosures
 - .3 Peripheral devices, Sensors, and accessories
 - .4 Keypads
 - .5 Power supplies

1.5.2. Intrusion System Performance requirement

- .1 Control Panel - The control panel is an eight (8)-partition, UL commercial burglary control panel that supports up to 128 zones using basic hardwired, polling loop, and wireless zones. It also provides supervision of the alarm bell output, RF receivers, and relay modules. In addition, ensure the controller provide the ability to schedule time-driven events, and allow certain operations to be automated by pressing a single button. The system interfaces a long-range radio unit that can send Contact ID messages and alphanumeric paging devices. The system is a Burglary System that includes the following functions:
 - .1 Basic Hardwired Zones - The control provides nine (9) hardwire zones with the following characteristics:
 - .1 EOLR supervision: supports N.O. or N.C. sensors (EOLR supervision required for UL installations).
 - .2 Individually assignable to one of the partitions.
 - .2 Optional Expansion Zones
 - .1 Polling Loop Expansion – Ensure control support up to 24 additional hardwire zones using built-in two-wire polling (multiplex) loop interface. The polling loop provides power and data to remote point modules and constantly monitor the status of all zones on the loop. The polling loop zones have the following characteristics:
 - .1 Interface with Remote Point Module devices
 - .2 Individually assignable to one of eight (8) partitions.
 - .3 Supervised by the control panel.
 - .4 A 12,000 ft (3658 m) wire runs without using a shielded cable.
 - .5 Each RPM (Remote Point Module) enclosure is tamper protected.
 - .3 Wireless Expansion – Ensure the control support wireless zones and the wireless zones have the following characteristics:

- .1 Supervised by control panel for check-in signals (except certain non-supervised transmitters).
- .2 Tamper protection for supervised zones.
- .3 Individually assignable to one of eight (8) partitions.
- .4 Support wireless devices listed for Commercial Burglary using RF Receiver.
- .4 Partitions – Ensure control provide the ability to operate eight (8) separate areas, each functioning as if it had its control. Partitioning features include:
 - .1 A Common Lobby partition (1-8), which can be programmed to perform the following functions:
 - .1 Arm automatically when the last partition that shares the common lobby is armed.
 - .2 Disarm when the first partition that shares the common lobby is disarmed.
 - .3 A Master partition (9), used strictly to assign keypads to view the status of all eight (8) partitions at the same time (master keypads).
 - .4 Assignable by zone.
 - .5 Assignable by keypad.
 - .6 Assignable by relay to one or all eight (8) partitions.
 - .7 Ability to display fire and/or burglary and panic and/or trouble conditions at all other partitions' keypads (selectable option).
 - .8 Certain system options are selectable by partition, such as entry/exit delay and subscriber account number.
- .5 User Codes – Ensure the control accommodates 250 user codes, all of which can operate any or all partitions. Certain characteristics must be assignable to each user code, as follows:
 - .1 Authority level (Master, Manager, or several other Operator levels). Each User Code (other than the installer code) is assigned the same or a different level of authority for each partition that it operates.
 - .2 Opening/Closing central station reporting option.
 - .3 Specific partitions that the code can operate.
 - .4 Global arming function (to arm all partitions the code has access to in one command).
 - .5 Use of an RF (button) to arm and disarm the system (RF key must first be enrolled into the system).
- .6 All exterior door magnetic contacts are triple-biased and highly resistant to defeat by external magnets.
- .7 Peripheral Devices – Ensure the control support up to 30 addressable ECP devices, which can be any combination of keypads, RF receivers, relay modules, annunciator modules, and interactive phone modules. Peripheral devices have the following characteristics:
 - .1 Each device is set to an individual address according to the device's instructions.
 - .2 Each device is enabled in-system programming.
 - .3 Detection and Alarm
 - .4 Each device's address is supervised (via a programming option)

- .8 Keypad/Annunciator – Ensure the control accommodates up to 16 keypads or six (6) touch-screen (i.e.; advanced user interface) keypads. Ensure keypads are :
 - .1 Performing all system arming functions.
 - .2 Be assigned to any partition.
 - .3 Provide four programmable single-button function keys, which can be used for:
 - .1 Panic Functions – activated by wired and wireless keypads; reported separately by partition.
 - .2 Keypad Macros – 32 keypad macro commands per system each macro is a series of keypad commands).
- .9 Optional Output Relays – A total of 96 relay outputs is accommodated using relay modules. Each relay module provides four (4) Form C (normally open and normally closed) relays for general purpose use or two (2) Class-B, Style-Y supervised notification appliance circuit outputs. The relays are:
 - .1 Programmed to activate in response to system events.
 - .2 Programmed to activate using time intervals.
 - .3 Activated manually.
 - .4 Assigned an alpha descriptor.
 - .5 Used for Class B, Style-Y supervised bell outputs.
- .10 Optional Interactive Phone Module – The control support remote access which permits access to the system to obtain system status information, Arm and disarms the security system and control relays.
- .11 Optional LED Annunciator – The control support annunciators that visually identify a zone or point that is in alarm or trouble.
 - .1 Commercial Wireless Equipment – The Control are compatible with UL Listed Commercial Wireless Fire & Security equipment and receive as many points as the control panel is rated for. Receivers may be remotely located anywhere on the system.
 - .2 Event Log – Ensure the System maintain a log of different events. The event log provides the following characteristics:
 - .1 Stores up to 1,000 events.
 - .2 Viewable at the keypad or through the use of a central management station.
 - .3 Printable on a serial printer.
 - .4 Stores access control events.
 - .5 Sends printed events to up to eight (8) alphanumeric pagers.
 - .3 Scheduling – Provides the following scheduling functions:
 - .1 Open/close schedules (for control of arming/disarming and reporting).
 - .2 Holiday schedules (allows different time windows for open/close schedules).
 - .3 Timed events (for activation of relays, auto-bypassing and bypassing, Auto-arming and disarming, etc.).
 - .4 Access schedules (for limiting system access to users by time)
 - .5 End-User Output Programming Mode (provides 20 timers for relay control).

- .6 The system automatically adjusts for daylight savings time.
- .4 Communication Features - Supports the following formats and features for the primary and secondary central station receivers:
 - .1 Formats
 - .1 Low speed to high-speed major formats
 - .2 Backup reporting – The system support backup reporting via the following:
 - .1 Secondary phone number.
 - .2 Long Range radio interface.
 - .3 Internet reporting – The system communicates with the central station via the internet. Ensure it provides the user with the ability to control the system via a browser interface. All packet data transmitted to the monitoring station is encrypted.
- .5 Audio Alarm Verification Option – Provides a programmable Audio Alarm Verification (AAV) option that can be used in conjunction with an output relay to permit voice dialog between an operator at the central station and a person at the premises.
- .6 Cross-Zoning function - Helps prevent false alarms by preventing a zone from going into alarm unless its cross-zone is also faulted within 5 minutes.
- .7 Pager Interface – The Control Panel sends event information to an alphanumeric pager via a pager interface device.
- .8 Exit Error False Alarm Prevention Feature – The System differentiates between an actual alarm and an alarm caused by leaving an entry/exit door open. If not subsequently disarmed, the control panel:
 - .1 Bypass the faulted E/E zone(s) and/or interior zones and arm the system.
 - .2 Generate an Exit Error report by a user and by zone so the central station knows it was an exit alarm and who caused it.
- .9 Programming – Ensure the Control is programmed locally or remotely
- .10 Panel Linking – The Control is networked together with other controls and being operated by any keypad within the system. It provides the ability for users to control multiple zones, partitions, and/or buildings from a central location, check status, and arm and disarm any partition from any keypad in the system, and Globally arm or disarm partitions based upon user authority.
- .11 Automation Software – The Control interface with automation software via an RS232 input on a single partition.

1.5.3. System Function Requirements

- .1 Regulate and monitor access at system-controlled doors.
- .2 Monitor connected detectors (supervised and auxiliary inputs) with the ability to manually or automatically arm and disarm them.
- .3 Control event initiated devices connected to system outputs, such as alarms or video recorders, with the ability to automatically or manually arm or disarm them.
- .4 Report an alarm condition.
- .5 Distribute and annunciate detailed zone-specific and system trouble alarm conditions via the internet, Plain Old Telephone Service (POTS), GSM/GPRS, and email notification to remote Alarm Monitoring Stations.

- .6 Establish a hierarchy of alarm types to prioritize handling alarm conditions.
- .7 Maintain a comprehensive database recording all site activity.
- .8 Integrate with a Video Surveillance system.
- .9 The Intrusion Detection system provide the ability to define local intrusion zones that consist of
 - .1 One or more access control readers
 - .2 One or more alarm inputs
 - .3 An input point to designate for arming and disarming
 - .4 An output point to designate for arming and disarming
- .10 The Intrusion Detection system provide the ability to arm or disarm intrusion zones by
 - .1 Keypad
 - .2 Access control reader, using card and keypad
 - .3 Digital Input state change
 - .4 Manual Operator control
- .11 Where the Intrusion Detection system is integrated with an access control system the Intrusion Detection system provides the ability to arm or disarm intrusion zones from outside the protected area.
 - .1 Readers assigned to an armed intrusion zone deny access to cardholders unless the intrusion zone is disarmed.
 - .2 Readers assigned to an intrusion zone flash LED indicators on the reader to annunciate the intrusion zone status.
 - .3 Cards authorized as to which intrusion zones they can arm and disarm.
 - .4 Users of the system enter keypad information to tell the system to arm or disarm and then they present their card
 - .5 If the user is authorized to arm zone, and they have active access right for the reader, then the intrusion zone is armed and any readers associated with the intrusion zone (other than the arm/disarm reader) is placed offline, any inputs associated with the intrusion zone is monitored on. An output is able to be generated based on the arm event. A history record is generated for this event.
 - .6 A configurable time delay before arming a zone exists allowing the user to leave the monitored area before the zone is armed.
 - .7 If the user is authorized to disarm the intrusion zone, and they have active access right for the reader, then the intrusion zone is disarmed and all readers associated with the intrusion zone return to normal operation, any inputs associated with the intrusion zone is monitored off. Ensure an output is generated based on the disarm event. A history record is generated for this event.
 - .8 If the user is not authorized to disarm the intrusion zone, but the user has an active access right for the reader, then access is denied, and a history record is generated.
- .12 The Intrusion Detection system provides the ability to arm or disarm intrusion zones by manual control
 - .1 A properly permissioned operator is able to manually arm or disarm an intrusion zone

- .1 Intrusion zones is partitioned to limit restrict which operator can view which intrusion zones.

- .13 Building Integration

- .1 The system integrates multiple buildings within one collective alarm monitoring entity whether the buildings are in relative proximity or at distant locations. The system's design further allows expansion or modification within existing buildings or the integration of new buildings at any time.
- .2 The system is structured to provide a continually expandable growth path for functions and features specified within this document without the necessity of exchanging previously installed controllers or software.

2. Products

2.1. CONTROLLERS

2.1.1. Controller

- .1 Minimum 8 zones on main control panel
- .2 Supports minimum 8 hardwired keypads
- .3 Expandable up to minimum 128 zones using hardwire, wireless modules, and addressable zones
- .4 Bus hardwired expansion
- .5 Minimum 8 partitions
- .6 Minimum 1,500 user codes (4 or 6 digits)
- .7 Minimum 3,000-event buffer
- .8 Minimum 9 accounts and 3 phone numbers
- .9 Minimum 1 supervised bell zone
- .10 Built-in telephone line and siren supervision
- .11 Auto SIA and Contact ID formats
- .12 Supports multiple types of alarm communicators
- .13 Full upload/download support with system download software
- .14 Complete with power supply modules as required Controller
- .15 Complete with zone expanders as required
- .16 Approval Listings: FCC/IC, UL/ULC
- .17 Approved Manufacturer: DSC or equivalent

2.1.2. Modules

- .1 Programmable Input Module
- .2 Programmable Output Module
- .3 Wireless Telephone Interface & Automation Control Module: As required
- .4 TC/IP Integration Module IT: As required

2.2. CONTROLLER ENCLOSURES

- 2.2.1. All controller enclosures are provided to house all controllers.

- 2.2.2. All controller enclosures are a single key locking metal box.
- 2.2.3. Size as required
- 2.2.4. Equipped with door tamper switch. Connect each door tamper switch to the intrusion detection system.
- 2.2.5. Ensure quantity and size of controller enclosures not exceed the real estate provided for mounting controller enclosures. Refer to contract drawings and coordinate as such.

- 2.3. COMMUNICATORS
 - 2.3.1. Internet/Intranet Alarm Communicator: as required
 - 2.3.2. GSM/GPRS Wireless Alarm Communicator: as required
 - 2.3.3. Internet and GSM/GPRS Dual-path Alarm Communicator: as required
 - 2.3.4. Provide communicators as required

- 2.4. PERIPHERAL DEVICES, AND SENSORS
 - 2.4.1. Magnetic Contacts (Steel)
 - .1 1" dia. contact for use in steel doors.
 - .2 Flush or surface mount as required
 - .3 Self-lock mounting
 - .4 Rugged Construction
 - 2.4.2. Magnetic Contacts (Wood)
 - .1 3/4" dia. contact for use in wood doors.
 - .2 Flush or surface mount as required
 - .3 "Wings" protect contact reed from being crushed from swelling wood
 - .4 Superior false alarm immunity
 - 2.4.3. Magnetic Contacts (Overhead Door)
 - .1 Miniature and low-profile design
 - .2 Stainless steel armored cable for added security and reliability
 - .3 Aluminum bar stock to resist corrosion in harsh environments
 - .4 Floor or track mount as required
 - 2.4.4. Glass Break Detectors:
 - .1 Acoustic glass break detectors with latching LED.
 - .2 Surface or wall mounted for an attractive and unobtrusive appearance.
 - .3 Minimum 7.62 M (25'-0") detection range and range measured to the furthest point on all types of glass.
 - .4 Fixed or adjustable detection angle 1- 360-degrees as required for complete coverage of all glass.
 - .5 Point to point and to the respective controller interface.
 - .6 Powered from centralised power supply.
 - 2.4.5. Passive Infrared Motion Detector

- .1 Ability to mask or orient to minimize the likelihood of nuisance alarms caused by environmental conditions.
- .2 Wired point to point and to the nearest controller interface.
- .3 PIR sensitivity adjustment
- .4 Adjustable detection range as required
- .5 Form 'A' or 'C' alarm contact and tamper switch
- .6 Pet immunity
- .7 Tamper-proof
- .8 Ceiling or wall mount as required.
- .9 Powered from centralised power supply.
- 2.4.6. Glass Break Detector and Passive Infrared Motion Detector Unit
 - .1 Integrated RF immunity motion detector
 - .2 Integrated glass break sensor
 - .3 Static and transient sensing
 - .4 Multi-Level Signal Processing
 - .5 Multi-element PIR sensor
 - .6 Temperature compensation
 - .7 Fast/Slow detection settings
 - .8 Quiet operation Glass break Detection
 - .9 Microcontroller-based Digital Signal Processing technology
 - .10 Dynamic Signal Processing
 - .11 Accurate detection of plate, laminated, wired and tempered glass types
 - .12 Reject common "bell" or "ringing" type sounds
 - .13 White noise rejection
 - .14 Installer test mode
 - .15 DSC BV-502GB or equivalent
 - .16 Provide Glass Break Detector and Passive Infrared Motion Detector Units at all glazing that is accessible from grade and as shown on drawings
- 2.4.7. Shock Sensor
 - .1 Unique bi-coloured LED to indicate minor or major attacks
 - .2 Anti-tamper protection
 - .3 Moisture-resistant electronics module
 - .4 Sensitivity adjustment
 - .5 High immunity to low-frequency false alarms and radio interference
 - .6 Compatible with all makes of controllers
 - .7 Able to monitor for minor vibrations (and count them to a pre-set limit) and for major attacks at the same time
 - .8 Approval Listings: FCC/IC
- 2.4.8. Request to Exit Detector
 - .1 Tyco Model T.REX-XL2-NL or approved equivalent.

2.4.9. Keypads

- .1 Programmable message LCD Keypad
- .2 are able to coexist with multiple (quantity as required) other keypads on a single system or controller
- .3 Large, backlit, with minimum 2-line, minimum 32-character display
- .4 Plain-language display of zone status, system status, trouble conditions, event buffer, system instructions, date and time
- .5 Ready, Armed and Trouble LEDs
- .6 Minimum 5 programmable function keys
- .7 Minimum 4 keypad-activated alarms: Panic, Auxiliary, Fire, and Duress
- .8 Backlight boost
- .9 Approval Listings: FCC/IC, UL/ULC
 - .1 ULC Commercial Burglary
 - .2 ULC Commercial Fire Monitoring
 - .3 ULC Residential Burglary
 - .4 ULC Residential Fire
 - .5 ULC Financial Burglary Certificate

2.4.10. Power Supply

- .1 Power supplies include all controller power supplies, all-electric lock power supplies, and all peripheral device power supplies.
- .2 All power supplies for controllers and peripheral devices provide a backup battery for up to three hours of operation upon loss of AC power. The controller retains database information for up to seven days upon loss of power.
- .3 Agency Listings
 - .1 UL Listed for Access Control Systems (UL294),
 - .2 Power Supplies for use with Burglar-Alarm Systems ULC-S318
 - .3 Hospital Signaling and Nurse Call Equipment (UL1069),
 - .4 Power Supplies for Fire Protective Signaling Systems (UL1481),
 - .5 CUL Listed - CSA Standard C22.2 NO. 205-12, Signal Equipment.
- .4 Features/Specifications
 - .1 Voltage: output as required.
 - .2 Amperage: Rating as required.
 - .3 Class 2 Rated power limited outputs.
 - .4 PTC (Positive Temperature Coefficient) protected outputs.
 - .5 Fuse rating as required
 - .6 115VAC 60Hz, input.
 - .7 Filtered and electronically regulated outputs.
 - .8 Short circuit and thermal overload protection.
 - .9 Built-in charger for sealed lead acid or gel-type battery backup.
 - .10 Zero voltage drop upon transfer to battery backup.

- .11 AC input and DC output LED indicators.
- .12 AC fail supervision.
- .13 Low battery and battery presence supervision.
- .14 Fire alarm system interface

3. Execution

3.1. COORDINATION

- 3.1.1. Engage a factory-authorized service representative to supervise and assist with startup service. Complete installation and startup checks in accordance with manufacturer's written instructions.
- 3.1.2. Coordinate all installations with related trades.
- 3.1.3. Related work required to be provided:
 - .1 Communications (IT)
 - .2 Electrical Works
 - .3 All 120 Volt wiring and connections from power panels to terminal strips in electronic low-voltage panels, power supplies, and devices A
- 3.2. CONTROLLERS AND PERIPHERAL DEVICES
 - 3.2.1. Ensure all Controllers, Controller enclosures, Communicators, Peripheral Devices, Sensors, and Keypads are installed and configured following manufacturer's installation instructions and recommendations, as per the Owners' requirements and as per contract drawings and specifications.
 - 3.2.2. Coordinate the exact mount location of all Controllers, Controller enclosures, Communicators, Peripheral Devices, Sensors, and Keypads to ensure that all conduits and back boxes are installed in the optimal locations.
 - 3.2.3. Coordinate exact mounting locations of all controllers and devices on-site with the Security Engineer's Representative and Owner.
 - 3.2.4. Provide all Controllers, Controller Enclosures, Communicators, Peripheral Devices, Sensors, and Keypads where indicated on contract drawings and documents and as required for a complete and operational intrusion detection system.
 - 3.2.5. All Controllers, Controller Enclosures, Communicators, Peripheral Devices, Sensors, and Keypads are inter-compatible.
 - 3.2.6. Submit shop drawings of all Controllers, Controller Enclosures, Communicators, Peripheral Devices, Sensors, and Keypads to the Security Engineer's Representative for approval before procurement and installation.
 - 3.2.7. Allow for "needs assessment sessions" with the Owner to determine the exact mode of operation for each Controller, Controller enclosure, Communicator, Peripheral Device, Sensor, and Keypad.
 - 3.2.8. Configure each Controller, Controller Enclosure, and Communicator, Peripheral Device, Sensor, and Keypad to suit the Owners' requirements.

3.3. POWER SUPPLY

- 3.3.1. System Power – The Intrusion Alarm System operate using standard 120 volts AC, 50/60 Hz power.
- 3.3.2. Supply and install power supplies as required for a fully functional intrusion detection system. Power supplies include all controller power supplies, all peripheral device power supplies.
- 3.3.3. Ensure systems have a minimum of Control Primary Power and Backup Battery. The battery is able to support the system and devices for 24 hours of continuous operation.
- 3.3.4. The battery input, auxiliary, and alarm outputs are protected using PTC circuit breakers. All outputs are power limited.
- 3.3.5. All power supplies are installed to manufacturer's recommendations and as required to furnish a fully functional intrusion detection system

3.4. INSTALLATION

- 3.4.1. Install the wiring system and integrate the system as indicated in this specification.
- 3.4.2. All equipment is wall-mounted with sufficient clearance to meet all applicable codes and facilitate observation and testing. All equipment is securely fastened with appropriate fittings to ensure positive grounding and be free of ground loops.

END OF SECTION

28 23 00.00 Video Surveillance

1. General

1.1. PURPOSE

- 1.1.1. The building's and facility's Network Video Management System's primary function is to protect the assets. The contents of this document are critical and are considered confidential. Ensure this information is not disclosed to anyone other than authorized personnel.
- 1.1.2. The Network Video Management Systems (NVMS) system, cameras, and accessories form part of the overall security strategy implemented and the system provide real-time video surveillance, recording of real-time events and historical video data for video evidence of a security event; and to provide a deterrent throughout the facility.

1.2. SCOPE OF WORK

- 1.2.1. The work covered by this section includes the furnishing, installation, and activation of all equipment & materials associated with provision of a complete turnkey NVMS as specified herein. This work may include integration with the associated subsystems and components listed in these sections.
- 1.2.2. Provide new equipment, cabling, devices, software, hardware, licences, integration with other systems, testing & commissioning.
- 1.2.3. The requirements of the conditions of the Contract, Supplementary Conditions, and General requirements apply to the work specified in this section.

1.3. SYSTEM REQUIREMENT

1.3.1. General

- .1 The security video system is an IP network-based, fully distributed digital video system. The security video system utilizes local area networks (LAN) as a transmission medium for video, configuration, as well as storage of all data. The security video system provides full video control at a control station, with additional full selection at any point within the network from a central management station. The security video system provides unlimited expansion for the addition or modification of video inputs. The system design is based on a Network Video Surveillance system and components.
- .2 Provide all security video cameras, pan/tilt/zoom (PTZ) cameras, mounts, housings, power supply systems, network cables, connectors, equipment racks, monitors and consoles, computer-controlled network switchers, central management stations, network video recorders, encoders, decoders, displays, and all other hardware and software to provide a fully operational system.

1.3.2. Video Management System Performance Requirements

.1 Configurations

- .1 Ensure the network video management system is an integrated hardware and software platform that serves as the Video Surveillance system management tool. The Video Surveillance system is an Internet Protocol (IP) based system complete with IP Video Surveillance cameras, Network Video Recorders (NVRs), Video Surveillance System Server, Video Surveillance System Video Management Owner, and Server Software to facilitate management of all NVRs and Video Surveillance cameras as well as to facilitate viewing of all video

stream for all Video Surveillance cameras from multiple central management stations via a TCP/IP data network.

.2 Basic architecture

.1 The system is optionally integrated with Security Management System (SMS). The TCP/IP network interconnects cameras, servers and Stations, and associated equipment.

.3 Integration with Security Management System

.1 The NVMS is integrated with Security Management System for building management and security-related applications and provide the following:

- .1 Alarms and events initiate recordings. These recordings show what happened before an alarm/event occurred.
- .2 The NVMS shares the SMS user interface (Station)
- .3 Users can view the NVMS videos on any Station on the network.
- .4 NVMS uses SMS security features to define each operator's viewing rights.
- .5 The NVMS system alarms and events are automatically sent to SMS or for inclusion in the Alarm and Event Summaries.
- .6 Recordings associated with SMS alarms and/or events can be viewed directly from the SMS Alarm or Event Summary.
- .7 An operator Station can control dedicated surveillance monitors.
- .8 Alarms can be associated with video content and displayed on video alarm monitors.

.4 NVMS integrate with legacy Video Surveillance equipment or take full advantage of open TCP/IP network technologies to deliver software-based camera switching, control, and digital recording. The NVMS have an open architecture and integrate with third-party products and applications.

.5 NVMS have a redundant configuration where video streams are redirected in the event of failure to minimize disruption and ensure uninterrupted recording.

.6 The user interface

.1 NVMS includes an easy-to-use Web-based interface that runs on standard computers. The video displays accesses using either Station or Internet Explorer.

.7 Network architecture options

.1 The NVMS utilizes a Conventional design that has no physical or logical protection between the various types, VLAN, and a network dedicated to security system

.8 NVMS Data Transmission

.1 The NVMS utilizes both Multicasting and Unicasting transmission techniques

.9 Network management

.1 The NVMS have as a minimum an appropriate set of network management tools that provide information such as Network utilization, Warning if utilization reaches a user-defined threshold, and Notification if a switch fails.

.10 Security

- .1 Ensure NVMS provide a range of security features, and supports both domain and workgroup security. The NVMS support internet explorer security, operator-based security, and central management station-based security.
- .11 VIDEO Management System (NVMS) servers
 - .1 The NVMS system servers store the configuration and runtime information of the system, distribute status information to the clients, accepts requests from the clients to view video, connects to video sources, transmit video from the cameras to the clients and store recorded video.
- .12 Recording Parameters
 - .1 The Video Surveillance system including the Video Surveillance system server and network video recorders are sized, equipped to record all video streams from all Video Surveillance cameras continuously at:
 - .2 Frames Per Second: 7
 - .3 Resolution: 2MP
 - .4 Compression: H.264 or H.265 (Good Quality)
 - .5 Recording: 100%, on motion 7 days per week. Assume 12 hours of motion per day 7 days per week
 - .6 Retention Days: 90
 - .7 Image Complexity: 50 - Average
 - .8 Motion %: 50 - Medium
 - .9 Spare capacity: 25%
- .13 Custom applications and scripts
 - .1 The NVMS allow custom applications and scripts to integrate with other applications.
- .14 Supporting video intercoms
 - .1 The NVMS support intercom functionality.

1.3.3. Central Management Station Performance Requirements

- .1 Ensure the central management station are equipped with two digital video outputs, a USB keyboard, and a mouse. Ensure it displays up to 16 video streams simultaneously and process up to 30 high-quality frames per second (fps) per stream, 720p. The central management station includes an advanced software package, and it provides full access to operations through a user-friendly and highly intuitive graphical user interface. The central management station interface uses drag-and-drop operations, context menus, and tooltips to enable interactions. The central management station have sound, graphics, colour, and on-screen messages to provide ongoing feedback about user activity and system status, and it have on-screen PTZ control and device property control.
- .2 The central management station interface allow the user to view live video; control cameras; record video; search, playback, export video; and provide an interface for viewing cameras and alarms on maps. It allows for multiple monitor support. When multiple video images are displayed, the technology automatically provides the best video display frame rate for the selected cameras. Cameras can be assigned to a user-defined location or camera group. The locations or groups can then be used in the display, sorting, and selection of devices. Ensure the central management station have

- plug-and-play installation and detection of cameras and devices, and have powerful script management and programming interface.
- .3 The central management stations allows users with authority to configure devices, set up users, adjust network settings, view system logs, and diagnostics, and create recording schedules. Permission to access these functions and all other system services can be configured to a fine level of detail.
 - .4 Ensure the central management station have advanced search functions, event logging, and alarm interface displays.
 - .5 The central management station export video and still images in multiple formats, including proprietary, G64, MP4, ASF, AVI, Pelco Native, QuickTime MPEG-4, Native MPEG-4, PNG, BMP, and JPEG. A front-panel USB port and DVD/CD-RW drive make it easy to export video clips and still images to external media. All proprietary formats have an appropriate file for viewing video and still images.
 - .6 The system provides user-defined workspaces on any central management station, based on an individual user profile.
 - .7 The central management station Application support the functionality to program scripts; these scripts are triggered to appear during a certain event and can be used to provide detail written or verbal instructions to the operator as to the actions to be taken.
 - .8 The central management station Application supports digital zoom on any fixed or PTZ cameras' video stream.
 - .9 The central management station Application provides the ability to control and program any camera equipped with pan, tilt controls, and zoom lens:
 - .1 Manually control the pan, tilt, and lens functions.
 - .2 Set the pan and tilt home positions for manual or alarm activation.
 - .3 Automatically control the cameras through an alarm trigger.
 - .4 Ability to set multiple pre-set positions.
 - .5 Ability to set multiple tours.
 - .6 Adjust the zoom lens.
 - .7 The ability to control the camera menu and set up the camera through the central management station.
 - .10 The system provides synchronized quad-screen playback with each quadrant playing video from different cameras all with the same time/date stamp.

1.3.4. System Function Requirements

- .1 Provided equipment, wiring, and other materials for a complete turnkey Video Surveillance system as shown and as specified. The systems are modular and expandable to an unlimited number of cameras.
- .2 The system consists of state of the art interior and exterior IP dome Video Surveillance cameras c/w lenses as required to facilitate the required field of views, local or remote power supplies, camera mounts as required, dome housing, dome housing complete with blower and heater, wiring, Power Over Ethernet (POE) Data switches, Network Video Recorders, Video Surveillance System Servers, Video Management Owner and Server Software and associated licenses.
- .3 The Video Surveillance systems provides fully integrated NVRs and camera management interface for command and control video surveillance that supports the following functionality:

- .4 Support network connectivity to multiple NVRs, servers, and network-connected central management stations.
- .5 Ensure communications interface between the NVRs, servers and network-connected central management stations are via 10Mb/100Mb/1000Mb/10Gb Ethernet connectivity using industry-standard TCP/IP protocol.
- .6 The Video Surveillance systems provide multi-window video management consoles for real-time video device monitoring and control from any central management station. NVRs, cameras, and assigned pre-sets are displayed alphabetically and grouped by the facility in a navigation pane for easy operator access.
- .7 Operators are able to simultaneously view and control multiple live video cameras across multiple NVR units. Camera control are mouse-driven on-screen and support pan, tilt, zoom, iris, focus, and camera pre-set call-up functions.
- .8 Ensure Operators are able to perform quick recall video playback on any selected camera view to request the last 15sec, 30sec, 1min, 2min, 5min, or select from the last 4 events listed for the selected camera.
- .9 Ensure Operators are able to access and playback recorded video events with on-screen controls that support play forward, play reverse, fast forward, fast reverse, single frame advance, single frame reverse, pause, stop, and variable speed control functions.
- .10 Ensure Operators are able to playback tagged video events stored locally on NVR units, based on date, time, alarm, event, text, and motion search queries from an embedded history/archive database.
- .11 Ensure Operators are able to save still image snapshots to file in the jpg file format from any live or recorded playback video stream.
- .12 Ensure Operators are able to save video clips to file in native or AVI file formats from any live or recorded playback video stream.
- .13 Ensure Operators are able to export evidence video clips to CDs or USB thumb drives with required media player.
- .14 The Video Surveillance system supports requests for live and recorded video transmission from NVR units at various resolutions and display sizes, independent of the actual NVR resolution setting for locally recorded video. Such a feature is user-configurable to facilitate network adaptability.
- .15 The Video Surveillance system allows the assignment of Video Surveillance cameras and pre-sets to Video Surveillance system alarm and card access events; for automating real-time camera control, automatic live video pop-up on alarm, video event tagging, and providing quick access to live and recorded video from any central management station.
- .16 The Video Surveillance systems provides simultaneous support for multi-vendor video drivers.
- .17 The Video Surveillance system monitors the status of all NVR units for processing and reporting Online / Offline status, Record status, Disk capacity status, Camera video loss, and Camera alarm.

2. Products

2.1. GENERAL

- 2.1.1. Where product model is specified and are deemed discontinued by the product manufacturer, provide the latest manufacturer recommend product model at the time of installation in leu of the specified model.
- 2.1.2. Where product performance specifications are provided, provide the latest manufacturer product model at the time of installation.
- 2.1.3. Exterior devices are sealed and protected against weather conditions including heat, cold, moisture, dust, and sand.
- 2.1.4. Commercial-grade, high quality, and rated for the environment in which it is being installed
- 2.1.5. Compatible with the video surveillance system.
- 2.1.6. All products and materials must be new and approved in the pre-installation submittals. Provide all equipment for a complete and operational IP-based Security Video Surveillance System Provide Owner with the necessary licenses as required for a complete and operational IP-based video surveillance system.

2.2. VIDEO SURVEILLANCE SYSTEM SERVER AND NETWORK VIDEO RECORDER AND SOFTWARE

- 2.2.1. Ensure Video Surveillance system server and network video recorder is a professional enterprise solution suited for commercial use and complete with the following features:

.1 Video

- .1 Real-time full-motion video (Min. 30fps per channel) minimum 48 video channels
- .2 Synchronous audio for every channel of video
- .3 Minimum 25 cameras can be viewed simultaneously from a single monitor
- .4 Multiple monitor / PC Decode feature output cameras to additional screens connected to your video card, both on the Server and Owner computer (Central Management Station)
- .5 MPEG-4, H.264 and H.265 compression technology
- .6 Live View: Real-Time up to 30fps per channel
- .7 Recording: Real-Time up to 30fps per channel
- .8 Records compatible Megapixel IP Cameras at up to 20MP.
- .9 Outputs software at up to 1920x1080 (1080P), as well as a TV or monitor which supports 1080P resolution.

.2 Software and Hardware

- .1 Multi-zone motion-detecting (entire frame or up to minimum detection zones per channel) with Privacy Mask option
- .2 Four recording modes: Continuous recording, Motion Detection, External Sensor, or Sensor/Motion
- .3 Alarm email message auto-sending with a photo attachment
- .4 SMS Text message auto-sending
- .5 Hardware watchdog support with auto-reboot
- .6 Position and colour-configurable OSD & Logo with Date/Timestamp

- .3 Digital Watermarks
 - .1 It is a requirement for all exported recordings and exported audit logs to be digitally signed. This is required to prove authentication (origin of the recording and audit log) and integrity (exported recording and audit log have not been altered or tampered with).
 - .2 The NVMS system provides a default digital certificate for signing the exported recordings and audit logs. Customization are also be provided to allow for the user to supply their digital certificate.
 - .3 A utility is provided to display the exported recording, view the audit log, and verify the digital signatures. A visual indication is provided as to whether the exported recording and audit log has been altered or tampered with.
 - .4 P/T/Z/F & Speed Dome control through software or keyboard - no additional hardware required. Protocols are as required to facilitate the complete operation of all Video Surveillance cameras.
- .4 Search/playback by date/time directory (random-access)
 - .1 Advanced Smart Search: only search footage within a designated area in playback mode instead of viewing countless hours of video
 - .2 Backup options include CD, DVD, USB, Network, Remote Backup, Blu-Ray
 - .3 Viewing live video
 - .4 Receiving and transmitting audio
 - .5 Recording administration
 - .6 Playing back recorded video
 - .7 Save recorded video sequences
 - .8 Export recorder video sequences (MPG, AVI, other)
 - .9 PTZ telemetry
 - .10 Alarm events
 - .11 SNMP Interfaces: system status, major alarms
 - .12 Sequence view of camera pre-set positions
 - .13 Modifying settings for a camera
 - .14 Modifying recording settings for a camera
 - .15 Adding and deleting cameras
 - .16 Creating schedules for recordings and video motion detection
 - .17 Modifying video motion detection settings and tuning
 - .18 Archiving mechanisms (automation of archiving)
 - .19 Report functions
 - .20 Network
 - .1 DDNS for dynamic IP addresses
 - .21 Remote access, administration, and recording on Owner computer through NVR Owner on LAN (network) or WAN (Internet)
 - .22 View multiple locations from one NVR Owner
 - .23 Bi-directional two-way remote communications between multiple NVR servers in various locations

- .24 NVR Owner's Compatible OS: Latest Windows OS including 64-bit compatibility with remote NVR Owner and or Linux OS.
- .25 Expansion / Options
- .26 Hybrid IP Camera Integration. Software and hardware support up to 64 total analogue and IP. Compatible with most major name brand IP cameras: any IP camera using latest ONVIF version.
- .5 Raid configuration
- .6 Fully configurable and task-oriented user interface
- .7 Multi-monitor support
- .8 Up to 10 user connections
- .9 Embedded reporting
- .10 Alarm management
- .11 Mobile access via latest windows client, Android and macOS Apps
- .12 Interactive graphical floor plan map of each facility
- .13 Security Encrypted communications between Owner and server
- .14 Configurable user and user group permissions and privileges
- .15 Authenticated user logins
- .16 User activity logs and audit trails
- .17 Digitally signed video recording (watermarking)
- .18 Rack Mount
- .19 Approved Manufacturers: Dell, HP
- 2.2.2. The NVMS software is:
 - .1 Genetec Omnicast™ Professional
 - .2 Avigilon Control Center Professional
 - .3 Milestone XProtect® Professional

2.3. KEYBOARD

- 2.3.1. The keyboard is used in conjunction with a complete network-based video system product, and it is the point from which all user functions can be accessed. The keyboard is USB compatible.

2.4. VIDEO SURVEILLANCE CAMERA TYPES

- 2.4.1. Approved manufacturers and models:

APPROVED MANUFACTURER	AXIS	HANWHA	BOSCH	VIVOTEK	AVIGILON
TYPE 1 MODEL	AXIS M3086-V	EQUIVALENT	EQUIVALENT	EQUIVALENT	EQUIVALENT
TYPE 2 MODEL	AXIS P4707-PLVE	EQUIVALENT	EQUIVALENT	EQUIVALENT	EQUIVALENT
TYPE 3 MODEL	AXIS M4327-P	EQUIVALENT	EQUIVALENT	EQUIVALENT	EQUIVALENT
TYPE 4 MODEL	AXIS M4227-LVE	EQUIVALENT	EQUIVALENT	EQUIVALENT	EQUIVALENT

2.5. POWER SUPPLY

2.5.1. Power supplies for Video Surveillance cameras are powered to a maximum of 80% load. Add power supply specifications meeting the project-specific requirement.

- .1 Indoor Single Camera Power Supplies
 - .1 Capacity – 4 Amps, (50VA)
 - .2 Output – 24 VAC output for 1 camera Fused output
 - .3 Input – 120 VAC input.
 - .4 Enclosure – Indoor
- .2 Indoor Multiple Camera Power Supplies
 - .1 Multiple cameras – 24/28VAC power supply unit and cabinet
 - .2 Output Capacity – 20 amp capacity
 - .3 Output – multiple camera circuits
 - .4 Enclosure – Surface NEMA /19" Rack mounted
- .3 Outdoor Camera Power Supplies
 - .1 Capacity – 4 Amps
 - .2 Output – 24/28 VAC for 1 camera.
 - .3 Input – 120 VAC or 230 VAC selectable input.
 - .4 Enclosure – NEMA 4/IP66 weatherproof

3. Execution

3.1. COORDINATION

3.1.1. Provide the following related work:

- .1 Communications (IT)
- .2 Electrical Works
- .3 All 120 Volt wiring and connections from power panels to terminal strips in electronic low-voltage panels, power supplies, and devices.
- .4 All raceway, conduit to the device(s), including all back boxes and pull strings, and the installation of all special back boxes.

3.2. CAMERAS AND ACCESSORIES

- 3.2.1. Provide and install camera housing and mounting accessories for the complete operation of the videos surveillance system.
- 3.2.2. Coordinate exact mounting locations of all cameras on-site with the Security Engineer's Representative and Owner.
- 3.2.3. Submit shop drawings to the Security Engineer's Representative for review before procurement and installation.
- 3.2.4. Allow for "needs assessment sessions" with the Owner to determine the exact camera settings.

3.3. POWER SUPPLY

3.3.1. Provide power supplies as required for a fully functional video surveillance system.

3.3.2. All power supplies are installed to the manufacturer's recommendations.

3.4. INSTALLATION

3.4.1. Provide all Video Surveillance system wiring, devices, and software as required for a complete and operational Video Surveillance System.

3.4.2. All camera installation, configuration, setup, program, and related work is performed by technicians thoroughly trained by the manufacturer in the installation and service of the equipment provided.

3.4.3. Provide all camera brackets as required for each camera's application.

3.4.4. Carefully follow instructions in documentation provided by the manufacturer to ensure all steps have been taken to provide a reliable, easy-to-operate system.

3.4.5. All equipment is tested and configured following instructions provided by the manufacturer before installation.

3.4.6. All firmware found in Video Surveillance System active devices is the latest and most up-to-date provided by the manufacturer.

3.4.7. All equipment requiring users to log on using a password is configured with user/site-specific password/passwords. No system/product default passwords are allowed.

3.4.8. Final camera viewing requirements to be determined by the Owner. Coordinate with the Owner and obtain viewing parameters for each Video Surveillance Camera. Adjust all Video Surveillance cameras to meet the Owner's requirements.

3.4.9. Adjust each Video Surveillance camera to obtain the best quality image or Video Surveillance camera image that is acceptable to the Owner.

3.4.10. All domes must have the password protection feature enabled to protect against unauthorized changes to dome programming. All PTZ domes are operated in continuous mode running an operator-defined pattern, pre-set tour, or combination pattern/pre-set tour. PTZ dome movement criteria are to be coordinated with the System Operator(s) and Design Engineer's Representative to ensure camera coverage meets defined needs. PTZ domes must be programmed for "auto-resume" after a pre-defined period and on power-up.

3.4.11. The Security Engineer's Representative conduct progress observations during construction to verify construction progress and verify the construction schedule. Coordinate progress observation site visits with the Security Engineer's Representative.

3.5. PROGRESS OBSERVATION

3.5.1. The Security Engineer's Representative conduct progress observations during construction to verify construction progress and verify the construction schedule. Coordinate progress observation site visits with the Security Engineer's Representative.

3.5.2. Security Conduit Rough-in and Preliminary Wire and Cable Installation

- .1 This observation intends to verify that adequate and proper conduit rough-in is installed, verify that wire and cable are being properly installed and labeled, and identify and resolve issues regarding conduit and wire and cable installation.

3.5.3. Preliminary Wire Termination Progress

- .1 This observation intends to verify that the installations and terminations to equipment are following specifications and standards.
- 3.5.4. Observations occur upon initial installation of each type of equipment (i.e. Panels, Card readers, alarm devices, junction boxes, etc.).
- 3.5.5. Observations must be complete before proceeding with the installation of remaining similar or like equipment.
- 3.5.6. Coordinate appropriate timing of each observation with the general contractor, Security Engineer's Representative as required to meet intended goals.
- 3.5.7. The reviewers issue reports for each observation to summarize findings and document clarifications noted during the observation.

END OF SECTION

28 26 00.00 Electronic Personal Protection System

1. General

1.1. PURPOSE

- 1.1.1. The Electronic Personal Protection System (EPPS) facilitates emergency communication between Duress-Panic Alarms and Emergency Phones Stations and Master Stations.

1.2. SCOPE OF WORK

- 1.2.1. Provide a complete turnkey EPPS.

- 1.2.2. The work covered by this section includes the furnishing, installation, and activation of all equipment & materials associated with complete IP-based EPPS as shown and as specified herein. This work may include, integration with the associated subsystems and components listed in these sections.

1.3. SYSTEM REQUIREMENTS

1.3.1. CONFIGURATION REQUIREMENTS

- .1 The EPPS are turnkey and provide a means for persons in duress to request assistance from monitoring locations that are equipped with master intercoms (emergency IP phones)/client workstation.
- .2 The EPPS consists of duress alarm stations that are electronically monitored. Each duress alarm station consists of but not be limited to a silent under desk button.
- .3 The duress alarm system facilitates instant locating of an activated duress alarm station. The location of the activated duress alarm station is displayed on a computer monitor via a "pop-up" graphical map of the parking respective lot as well as an alphanumeric unique name on each emergency IP phone.

2. Products

2.1. GENERAL

- 2.1.1. All equipment is rated for continuous operation. Environmental conditions (i.e. temperature, humidity, wind, and seismic activity) is taken under consideration at each facility and site location before installation of the equipment.
- 2.1.2. Ensure duress alarm system is installed, and programmed in a manner that allow for ease of operation, programming, servicing, maintenance, testing, and upgrading of the system.
- 2.1.3. Provide wire/cable recommended and approved by the OEM. Ensure Cabling meets the interconnecting wiring requirements of NFPA 70.
- 2.1.4. Systems are scalable and allow expansion as required.
- 2.1.5. All hardwired alarms, switches, and junction boxes are protected from tampering and include line supervision.
- 2.1.6. The installation and placement of devices in strategic locations also requires that signage be posted near these devices.

- 2.1.7. All system components are designed to provide continuous electrical supervision of the complete and entire system.
- 2.1.8. Ensure all alarm and initiating and signaling circuits is supervised for open circuits, short circuits, and system grounds. When an open, short or ground occurs in any system circuit, an audible and visual fault alarm signal is initiated at the master control station and all remote locations.
- 2.1.9. The system consists of the components to constantly monitor and verify alarm activation; identify zone of activation and location of activation.
- 2.1.10. Audible Signal Device for Duress: Provides alarm activation and audible sound for alarms, as well as supervisory and trouble signals that is distinctive.
- 2.1.11. Assessment: This ability consists of electronic devices required to visually and audibly verify the validity of alarms. The assessment also includes providing an indication of tampering, fail-safe, low battery, and power losses.
- 2.1.12. Panic Button:
 - .1 Potter Surface Mount HUB-M or approved equivalent.
 - .2 Mounted under desk as indicated on security floorplans
 - .3 Alarm to be silent and local to the facility only with capability to be relayed to the alarm monitoring company
- 3. Execution
 - 3.1. DEVICES
 - 3.1.1. Ensure all devices are installed, configured, and programmed following the manufacturer's installation instructions and recommendations, as per the Owner's requirements and as per contract drawings and specifications.
 - 3.1.2. Allow for needs assessment sessions with the Owner and configure the Blue Alert® MNS and Blue Alert® EMS Owner software as per the owner's requirements.
 - 3.1.3. Ensure all devices, software, firmware, and warranty are registered in the sole name of and is in the sole ownership of the Owner.
 - 3.1.4. Coordinate the exact mount location of devices on-site to ensure that all conduits and back boxes are installed in the optimal locations.
 - 3.1.5. Provide devices as indicated on contract drawings and documents.
 - 3.1.6. Provide all wiring as indicated on contract drawings and documents and as required to provide a complete turnkey duress alarm system.
 - 3.1.7. Ensure all devices are compatible with the duress alarm system.
 - 3.1.8. Submit shop drawings of all devices to the Security Engineer's Representative for approval before procurement and installation.
 - 3.1.9. Allow for "needs assessment sessions" with the Owner to determine the exact mode/s of operation of each and system
 - 3.1.10. Configure each device to suit the Owner's requirements.
 - 3.1.11. Provide power supplies as required for a fully functional duress alarm system.

3.2. INSTALLATION

- 3.2.1. Engage a factory-authorized service representative to supervise and assist with startup service. Complete installation and startup check in accordance with manufacturer's written instructions.
- 3.2.2. Install all system components and appurtenances following the respective manufacturer's specifications, referenced practices, guidelines, and applicable codes. Furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signal, communications, and data transmission line grounding are installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.
- 3.2.3. Provide, install and configure all equipment, wiring, software, and software licenses to provide all systems configuration requirements and all system performance requirements as indicated in this section.
- 3.2.4. Install the wiring system and integrate the system as indicated in this specification. All wiring is to be installed in a dedicated conduit throughout. Ensure wiring is not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with another building wiring.
- 3.2.5. All low voltage wiring is plenum rated where required by code.
- 3.2.6. Ensure all wiring conductors are individually numbered and each cable or wiring group being extended from a panel or cabinet to a building-mounted device is identified with the name and number of the particular device.
- 3.2.7. All exposed wiring inside and outside the control console, cabinets, boxes, and similar enclosures, are dressed down neatly and secured with wiring cleats or wire ties.
- 3.2.8. All cabinets, boxes, and similar enclosures containing security system components and/or cabling and are easily accessible to employees or the public is provided with a lock. Boxes above ceiling level in occupied areas of the building is not be considered to be accessible.
- 3.2.9. Ensure all junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public is covered with a suitable cover plate and secured with tamper-proof screws.
- 3.2.10. Riser diagrams are schematic and do not show every conduit, wire box, fitting, or other accessories. Provide such materials as necessary for a complete and functioning installation. Install following referenced codes and these specifications. Use weatherproof equipment or covers where installed in areas exposed to the weather.
- 3.2.11. All equipment is mounted with sufficient clearance to meet all applicable codes and facilitate observation and testing. Ensure all equipment are securely fastened with appropriate fittings to ensure positive grounding and be free of ground loops.
- 3.2.12. Determine conductor requirements for each device following the Contract Documents and manufacturer requirements.
- 3.2.13. Route wire and cable as required preventing interference and signaling contamination of both Security System cable and cable associated with other systems. Coordinate the routing of wire and cable requiring isolation from power, radio frequency (RF), telephone, etc.
- 3.2.14. Provide sleeves and code-compliant fireproofing techniques for all penetrations of fire-rated partitions, masonry walls, and slabs, where the penetrations are made by or used for installation of Security Systems.
- 3.2.15. Separate high voltage (120 VAC and above) cables from low voltage cables within enclosures

- 3.2.16. Run wire and cable continuously from the device location to the final point of termination. No mid-run cable splices are allowed
- 3.2.17. Bundle and tie wire and cable with cable ties.
- 3.2.18. Cover exposed high voltage (120 VAC and above) power terminations within DGP's, power distribution cabinets, and other security enclosures.
- 3.2.19. Ensure system installation is following NFPA 731 Standards for the Installation of Electric Premises Security Systems and appropriate installation manual for each type of subsystem designed, engineered, and installed.
- 3.2.20. Ensure the location and type of duress alarm station are following physical security requirements as shown in the security systems layout drawings.
- 3.2.21. Wall, column, and pole-mounted stations are mounted to meet AODA requirements and use tamper-proof bolts and screws.
- 3.2.22. Cleaning: After installation, clean each system component of dust, dirt, grease, or oil incurred during installation following the manufacturer's instructions.
- 3.2.23. Adjustment/Alignment/Synchronization: prepare for system activation by following the manufacturer's recommended procedures for adjustment, alignment, or programming. Prepare each component following appropriate provisions of the component's installation, operations, and maintenance instructions.
- 3.2.24. Upon project commencement, provide qualified technical personnel on-site. Personnel are present on each consecutive working day until the system is fully functional and ready to begin the testing phase of this project.
- 3.2.25. During the installation process maintain an up-to-date set of as-built shop drawings, which is always be available for review by the Owner and/or Engineer's Representatives. This set of documents should be annotated with as-built data as the work is performed. These documents are reviewed as part of the approval process when evaluating payment request applications. At a minimum, the drawings should contain the following information:
 - .1 Quantity and location of all equipment installed.
 - .2 Cable and wire run along with the designation tags assigned to each.
 - .3 Wiring diagrams that indicate terminal strip layout, identification, and terminations.
- 3.2.26. Maintain continuous coordination with the Engineer's Representatives. Ensure the engineers are kept informed of the progress and all conflicts that arise during this project.
- 3.2.27. Coordinate all proprietary intercom substation back boxes for rough-in.
- 3.2.28. All installation, configuration, setup, program, and related work is performed by technicians thoroughly trained by the manufacturer in the installation and service of the equipment provided.
- 3.2.29. Install all devices and wiring as recommended by the intercom system manufacture.
- 3.2.30. Coordinate with the Owner, configure and program the system as required to suit operations of the facility as directed by the Owner.
 - .1 Coordinate the exact mount location of devices to ensure that all conduits and back boxes are installed in the optimal locations.
 - .2 Submit shop drawings to the Security Engineer's Representative for review before procurement and installation.
 - .3 Ensure all power supplies are installed to the manufacturer's recommendations. Provide power supplies where not shown on drawings but are required for complete operating of

duress alarm stations. Provide all wiring from power supplies to each duress alarm station. All power supplies are centralized and located in the telephone room. Provide 120V 15A circuits from the electrical panel to power supplies.

- .4 Carefully follow instructions in documentation provided by the manufacturer to ensure all steps have been taken to provide a reliable, easy-to-operate system.
- .5 Ensure all equipment are tested and configured following instructions provided by the manufacturer before installation.
- .6 All equipment requiring users to log on using a password is configured with user/site-specific password/passwords. No system/product default passwords are allowed.

3.3. PROGRESS OBSERVATION

3.3.1. Ensure Security Engineer's Representative conduct progress observations during construction to verify construction progress and verify the construction schedule.

3.3.2. Security Engineer's Representative conduct the following minimum progress observations:

- .1 Security Conduit Rough-in and Preliminary Wire and Cable Installation
 - .1 This observation intends to review conduit rough-in, wires, and cables being installed and labeled, and identify and resolve issues regarding conduit and wire and cable installation.
- .2 Preliminary Wire Termination Progress
 - .1 This observation intends to verify that review the installation and termination of equipment and following specifications and standards.

3.3.3. Observations occur upon the initial installation of each type of equipment.

3.3.4. Observations must be complete before proceeding with the installation of remaining similar or like equipment.

3.3.5. Coordinate appropriate timing of each observation with the general contractor, Security Engineer's Representative as required to meet intended goals.

3.3.6. The reviewers issue reports for each observation to summarize findings and document clarifications noted during the observation.

END OF SECTION

28 40 00.00 Electronic Safety and Security Systems Integration

1. General

1.1. CONFIGURATION

1.1.1. The following systems are integrated on a single common IP network via respective servers; controllers and a common data switch to provide integrated functions as described in this specifications document and on Contract Drawings.

- .1 Access Control
- .2 Video Surveillance System
- .3 Intrusion Detection System
- .4 Intercom System

1.1.2. Personal computers (Referred to as Central Management Stations) is provided at locations indicated on contract drawings. Ensure each personal computer is equipped with all required, hardware, Owner and or server software; software licenses and facilitate remote administration of all systems as described in the contract documents.

1.1.3. The functions of each Central Management Station and video wall includes:

- .1 View, monitor, and administer security systems via interactive graphical maps of the facility.
- .2 Administration of credentials
- .3 View, monitor and administer video streams from each Video Surveillance camera
- .4 Display single and/or multiple video streams from multiple Video Surveillance cameras simultaneously
- .5 Functions described in all sections of these specifications
- .6 The systems are modular and expandable as herein specified or as the Owner may direct up to full system capacity.

1.1.4. All hardware, Owner and or server software; Ensure software licenses is provided and installed and configured on the Central Management Stations and video wall, all servers and controllers to facilitate the following integration of the electronic safety and security system indicated as "required" in the following Electronic Safety and Security Systems Integration Matrix.

	Access Control System	Video Surveillance System	Intrusion Detection System	Intercom System	Electronic Personal Protection System / Duress Alarm	3rd Party Alarm Monitoring Company	Fire Alarm System
Access Control System		Required	Required	Required	Required		Required
Video Surveillance System			Required	Required	Required		

Intrusion Detection System						Required	
Intercom System							
Electronic Personal Protection System / Duress Alarm							
3rd Party Alarm Monitoring Company							
Fire Alarm System							

- 1.1.5. Ensure all hardware, Owner and or server software; software licenses are provided and installed, and configured on the Central Management Stations, all servers, and controllers to facilitate the following integrated functions:
- .1 Access Control and Video Surveillance System
 - .1 Upon invalid card, forces entry at a secured door or door held open beyond pre-set acceptable duration, the access control system signals the Video Surveillance System to display the video streams from the Video Surveillance camera with a view of the respective door. The video stream is displayed immediately on each Central Management Station Monitor following the event. Ensure it is possible to display the video stream in full-screen format or reduces size format.
 - .2 Intrusion Detection System and Video Surveillance
 - .1 Upon activation of an intrusion alarm the intrusion detection system signals the Video Surveillance System to display the video streams from the Video Surveillance camera with a view of the activated alarm point. Ensure the video stream is displayed immediately on each Central Management Station Monitor following the event. It is possible to display the video stream in full-screen format or reduces size format.
 - .3 Access Control and Intrusion Detection System
 - .1 Upon activation of an alarm on the access control system it relays the alarm as a unique addressed alarm to the intrusion detection system. The intrusion detection system relays the alarm to 3rd party alarm monitoring company.
 - .2 Upon presentation of a valid credential at a designated credential (card) reader the access control system shall arm the intrusion detection system if the intrusion detection system is in a disarmed state.
 - .3 Upon presentation of a valid credential at a designated credential (card) reader the access control system shall disarm the intrusion detection system if the intrusion detection system is in an armed state.
 - .4 Access Control and Intercom System

- .1 Upon activation of a door/gate intercom substation, an operator has the ability to open the respective door by activating a door /gate release button on the answering master intercom station.
- .5 Access Control and Electronic Personal Protection System / Duress Alarm
 - .1 Upon activation of the Electronic Personal Protection System / Duress Alarm station, ensure the access control system logs the date and time of the even. The access control system also logs the date and time when the event was cleared/reset by an operator.
- .6 Video Surveillance and Electronic Personal Protection System / Duress Alarm
 - .1 Upon activation of the Electronic Personal Protection System / Duress Alarm station, the Electronic Personal Protection System / Duress Alarm signals the Video Surveillance system to automatically pop up and display video streams from the Video Surveillance cameras that are because of each activated Electronic Personal Protection System / Duress Alarm station.
- .7 Intrusion Detection System and 3rd Party Alarm Monitoring Company
 - .1 Ensure upon activation of an alarm on the intrusion detection system relay the alarm as a unique addressed alarm to the 3rd party alarm monitoring company.
- .8 Video Surveillance System and Intercom System
 - .1 Upon activation of a intercom system, the intercom system signals the Video Surveillance cameras because of the activated intercom station to pan and zoom to the area at and around the activated intercom station. The video stream from each Video Surveillance camera is then displayed immediately on each Central Management Station Monitor following the event.
 - .2 Upon activation of an intercom station, the video feed from the activated intercom station is displayed at the relative master video intercom station. The video feed from the activated intercom station is then recorded on the network video recorder.
- .9 Access Control System and Fire Alarm System.
 - .1 View in real-time all critical and fire events from the same interface via a unique alphanumeric identifier and customizable icon on the Central Management Station Monitor.
 - .2 Electronically Log all fire alarm activity and events in the security system event database for future investigation. Log to include activity and events name and description, date and time event occurred, dates and times event changed state, and date and time event was cleared.
 - .3 View in real-time fire panel event status for quick investigation a unique alphanumeric identifier and customizable icon on the Central Management Station Monitor.
 - .4 View in real-time AC power status, battery status, and more for quick troubleshooting via interactive icon and unique alphanumeric identifier on the Central Management Station Monitor
 - .5 Supports network panels using network servers
 - .6 View in real-time all fire alarm events on a graphical interactive map of the facility on the Central Management Station Monitor. All fire device alarm events are displayed via a unique alphanumeric identifier and customizable icon. Once events are cleared at the fire alarm system, the event status is automatically updated to "clear" on the graphical interactive map.

- .7 Upon activation of the fire alarm system, the fire alarm system triggers the automatic pop-up of operator-defined specific Video Surveillance camera video streams on the Central Management Station Monitor.

2. Product

2.1. GENERAL

- 2.1.1. Where product model is specified and are deemed discontinued by the product manufacturer, provide the latest manufacturer recommend product model at the time of installation in leu of the specified model.
- 2.1.2. Where product performance specifications are provided, provide the latest manufacturer product model at the time of installation.
- 2.1.3. All products and materials must be new and approved in the pre-installation submittals.
- 2.1.4. Ensure exterior devices are sealed and protected against weather conditions including heat, cold, moisture, dust, and sand.
- 2.1.5. Commercial-grade, high quality, and rated for the environment in which it is being installed
- 2.1.6. Compatible with the system.
- 2.1.7. Central Management Station computers
- 2.1.8.** Central Management Station computers complete with dual monitors, keyboard and mouse configured as follows:

MODEL:	DELL XPS 8910
PROCESSORS:	LATEST GENERATION INTEL® CORE™ I7 PROCESSOR (HIGHEST AVAILABLE CACHE AND HIGHEST AVAILABLE SPEED (GHZ)
MEMORY:	MINIMUM 24GB MEMORY
BOOT HARD DRIVES:	MINIMUM 2TB 7200 RPM SSD HARD DRIVE
REMOVABLE MEDIA STORAGE DEVICE:	DVD-RW DRIVE (READS AND WRITES TO DVD/CD)
VIDEO CARDS:	2 X NVIDIA® GEFORCE® GTX 750TI WITH 2GB GDDR5 GRAPHICS MEMORY
PRODUCTIVITY SOFTWARE:	MICROSOFT OFFICE HOME AND BUSINESS 2016
MONITORS:	2 X DELL ULTRASHARP™ 25 MONITOR - U2515H
USB PORTS:	MINIMUM 2
SECURITY SOFTWARE:	MCAFFEE LIVESAFE 36 MONTH SUBSCRIPTION
HARDWARE SUPPORT SERVICES:	3 YEAR PRO SUPPORT WITH 3 YEAR NBD LIMITED ONSITE SERVICE AFTER REMOTE DIAGNOSIS
MOUSE:	DELL USB 6-BUTTON LASER MOUSE
OPERATING SYSTEM:	LATEST PRO 64-BIT ENGLISH
SOFTWARE:	LATEST MICROSOFT OFFICE HOME AND BUSINESS

USER INTERFACE:	GRAPHICAL USER INTERFACE, WINDOWS-STYLE
VIDEO SYSTEM	PCI-E GRAPHICS CARD WITH MINIMUM OF 256 MB VIDEO RAM (NON-SHARED MEMORY), 1280 X 1024 DISPLAY RESOLUTIONS, AND DIRECTX 8.1 APPLICATION PROGRAMMING INTERFACE; TRUE COLOUR (32-BIT), TWO DIGITAL VIDEO OUTPUTS
AUDIO INPUTS	TWO 3.5 MM STEREO JACKS
AUDIO OUTPUTS	ONE 3.5 MM STEREO JACK
NETWORK SPECIFICATIONS:	INTERFACE GIGABIT ETHERNET RJ-45 PORT, (1000BASE-T)
WARRANTY:	3 YEARS HARDWARE SERVICE WITH ONSITE/IN-HOME SERVICE AFTER REMOTE DIAGNOSIS

2.2. KEYBOARD VIDEO MOUSE (KVM)

2.2.1. Tripp LiteB030-008-17-IP complete with all cables to connect all servers or approved equal.

3. Execution

3.1. INSTALLATION

3.1.1. Data Switches

- .1 Refer to the contract drawings and specifications, provide and configure all data core and edge switches as required to create an Internet Protocol (IP) local area network as indicated.
- .2 Create and configure all Virtual Local Area Networks (VLANs) as indicated on drawings and as indicated in the System Data Bandwidth Allocation Table below

System Data Bandwidth Allocation Table		
System VLAN	Bandwidth	Additional Requirements
Video Surveillance	Minimum as Required to ensure optimal performance of the Video Surveillance systems + 100% growth.	All Virtual Local Area Networks (VLANs) and respective Bandwidths are configured with Quality of Service (QoS) to ensure optimal performance of all voice, video and data services with maximum 40 millisecond latency.
Video Wall	As required to stream and display camera video streams simultaneously at 720P resolution 15 frames per second.	
Access Control	Minimum 3 MBS	
Intercom	Minimum 3 MBS	

AV	Minimum 10 MBS	
BAS	Minimum 2 MBS	
Lighting Control	Minimum 2 MBS	
Building Operations Network	Minimum 20 MBS + 100% growth	

- 3.1.2. Coordinate with the Audiovisual (AV), Building Automation System (BAS), and Lighting Control contractors; configure all data switches to facilitate complete connectivity and communications between all AV, BAS, and Lighting Control systems head-end and peripheral IP devices.
- 3.1.3. Provide all hardware, software, customized software, software licenses, wiring, and all patch cords as required to integrate all systems as described in the contract drawings and this electronic safety and security system specifications, as specified by the respective system manufacturers and as required by the Owner.
- 3.1.4. Provide all "required" wiring, hardware, software, customized software, and software licenses, coordinate with the Owner's Information Technology (IT) representatives, and make all physical and logical connections to the security system VLAN to enable integration of all security systems as described in the contract drawings and this electronic safety and security system specifications. "Required" includes all wiring, hardware, software, customized software, and software licenses that are specified and that are not specified but required to facilitate the integration of all security systems as described in the contract drawings and this electronic safety and security system specifications.
- 3.2. VIRTUAL SEPARATION OF SYSTEMS
- 3.2.1. A total of 7 user groups (business units) occupies contiguous and non-contiguous spaces throughout the facility.
- 3.2.2. Each user group requires a separate virtually segregated Access Control, Video Surveillance, and Intercom system.
- 3.2.3. The segregated systems facilitate autonomous operations of the security systems and security management.
- 3.2.4. Ensure one (1) master administrator group has access to and manage each Access Control, Video Surveillance, and Intercom system (A total of 3 master administrator groups).
- 3.2.5. Allow for coordination with the 7 user groups and the master administrator group and:
- .1 Configure the Access Control, Video Surveillance, and Intercom systems servers and, establish 7 virtual subsystems per Access Control, Video Surveillance, and Intercom system (A Total of 21 virtual subsystems).
 - .2 Determine the ownership of each Access Control, Video Surveillance, and Intercom systems device and assign each device to its respective virtual subsystem. Examples of system devices are video surveillance cameras, card readers, door contacts, electric strikes, motion requests to exit, Intercom substations, Intercom master stations, etc.
- 3.2.6. Provide the following for each virtual subsystem:
- .1 Secured virtual separation from all other subsystems
 - .2 User access via secured user login from client computers that are connected to the common building network

- .3 Ability for a user to monitor, manage and administer all devices and functions within their respective subsystem
 - .4 All other functionalities as indicated in the Electronic and Security Specifications document
- 3.2.7. Provide the following for each master administrator group:
- .1 User access to the Access Control, Video Surveillance, and Intercom system via secured user login from client computers that are connected to the common building network.
 - .2 Ability for a user to monitor, manage and administer all devices and functions within respective subsystem
 - .3 Ability to make changes to the system's configuration
 - .4 Access to all software features, functions and files
 - .5 Ability to add, delete or modify user access and privileges
 - .6 View or edit notes created by users.
 - .7 All other functionalities as indicated in the Electronic and Security Specifications document.
- 3.3. SOURCE CODES
- 3.3.1. The Owner becomes the owner of all proprietary and open source codes, software and programming developed under this project. Provide the Owner with all source codes, software, programming, configuration data and all relative passwords and keys developed and or generated under this project. Ensure the Owner has full and unhindered access to all source codes, software, programming, configuration data and all relative passwords and keys developed and or generated under this project.
- 3.4. CYBER SECURITY
- 1.1.1. Coordinate with Owner's Information Technology representatives, obtain a copy of Owner's cyber security policy and provide all applicable cyber security configurations. Definitions
 - 1.1.3. Cyber Assets: Systems (including hardware, software, and data) and communication networks (including hardware, software, and data).
 - 1.1.4. Critical Cyber Assets: Cyber assets that perform critical system functions. The loss or compromise of these cyber assets would adversely affect the operational reliability of the system.
 - 1.1.5. Cyber Attack: The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
 - 1.1.6. Cybercrime: Any crime where cyber – the internet and information technologies, such as software, firmware, computers, tablets, personal digital assistants or mobile devices – has a substantial role in the commission of a criminal offence.
 - 1.1.7. Cyber Hygiene: Practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.

- 1.1.8. Cyber Incident: Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.
- 1.1.9. Cyber Security: Technologies, processes and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.
- 1.1.10. Cyber Threat or Cyber Security Threat: Malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DDoS / DoS) attacks and other attack vectors.
- 1.1.11. Cyber Threat Actors: Broad term for any states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber Security awareness, and technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems and networks.
- 1.1.12. IP Multicast: Technique for one-to-many and many-to-many real-time communication over an IP Infrastructure network.
- 1.1.13. Endpoint: Remote computing device that communicates back and forth with a network to which it is connected. Such as a server, desktop, or laptop.
- 1.1.14. Network Certificates: Also known as a Digital Certificates, which are an electronic "password" that allows a person or organization to exchange data securely over the internet using the public key infrastructure (PKI). Digital Certificates are also known as a public key certificate or identity certificate. There are 3 Main types of certificates:
 - .1 Secure Socket Layer Certificate (SSL) Digi-SSL
 - .2 Software Signing (Code Signing Certificate) Digi-Code
 - .3 Client Certificate (Digital ID) Digi-ID
- 1.1.15. Social Engineering: Exploitation methods that target human vulnerabilities, such as carelessness and trust.
- 1.1.16. Technical Vulnerabilities: Weaknesses or flaws in the design, implementation, operation, or management of an information technology system, device, or service.
- 1.2. CYBER SECURITY MEASURES
 - 1.2.1. Implement at minimum the following multi-layered Cyber Security measures to limit and / or reduce the Owner's potential risk from a cyber threat event; such as a Cyber Security data breach or Cyber Security attack.
 - 1.2.2. Password Management
 - .1 Employ password management best practices such as:
 - .1 Do not use default passwords.
 - .2 Use strong and unique passwords for all applications. Use a minimum of 8 characters where there is no password policy inherent in the software; use a mixture of uppercase and lowercase letters, numbers, and include at least one special character (! @ # ?]).
 - .3 Reset passwords at regular intervals.
 - .4 Configure two-factor authentication for all accounts where possible in the system software.
 - .5 Do not use System Admin logins for simple tasks; create separate User accounts with rights levels appropriate for the job function. Create and define

user accounts as appropriate such as Role based, Individual logins or assigned roles.

- .6 Use different passwords for every account
- .7 Enforce secure password policies within the business environment.
- .8 Have interface lock after a predefined # of failed login attempts for a pre determined time interval.

1.2.3. Port and Interface Management

- .1 Employ Port Management techniques such as:
 - .1 Restrict access on network switch ports to assigned devices addresses.
 - .2 Lock down all open, unused and unsecure ports on the networking devices such as switches, routers, and firewalls.
 - .3 Shut off all unused communication services and hardware interfaces.
 - .4 Advise Owner on use of 3rd party port security monitoring.

1.2.4. Physical and Virtual Networks

- .1 Provide a dedicated VLAN for the network connected systems where a dedicated LAN has not been provided.

1.2.5. Encryption

- .1 Use minimum TLS 1.2 for all network attached equipment and use TLS 1.3 where available.

1.2.6. Network Certificates

- .1 Ensure Network Certificates are up to date and not expired for all equipment and systems.

1.2.7. Firmware & Software Update Management

- .1 Use the latest stable Firmware / Software version on all devices / equipment as well as implement a Firmware / Software Update management process and procedure.

1.2.8. Manufacturer's System Hardening Guides

- .1 Provide the Manufacturer's System hardening guides for the equipment being installed and implement as many recommendations / features as possible.

1.2.9. External Memory

- .1 Restrict the use of external memory. Restrict or eliminate the use of devices such as external USB Thumb drives unless expressly allowed by the Owner's Information Technology representatives.

1.2.10. Log Off

- .1 Enable auto-log off timer for all software, websites and logins. Set auto-log off timer on local central management station (s) being used to access the equipment with a reasonable timer in the case that an employee leaves the central management station unattended.

1.2.11. Anti-Virus Software

- .1 Enable and configure anti-virus software on PC endpoints in accordance with the Owner's Information Technology requirements, unless it is to be installed and configured by the Owner.

1.2.12. Filtering Techniques

- .1 Apply filtering techniques including the types listed below where possible:
 - .1 Web Filtering: A Web filter adds another layer to anti-phishing defences by blocking the web based component of phishing and malware attacks.
 - .2 Multicast Message Filtering: Filters the packets sent to multicast groups users are not subscribed to.
 - .3 Content Filtering: Is the use of a program to screen and / or exclude access to web pages or email deemed objectionable. Ensure a content filter is used to block access to this content.

1.2.13. Back up Regularly

- 1. Provide backup schedule in the closeout submittals and configure system for automatic backups wherever possible.
- 2. Identify files that require manual backup and the backup procedure. This helps to protect against many types of data loss, especially if a Cyber Threat Actor gains access.

1.3. IT DEVICES AND SYSTEMS

1.3.1. Apply the Cyber security measures listed in the clauses above in part or in full, as possible, to a wide range of Information Technology (IT) Devices including:

- .1 Firewalls
- .2 Routers
- .3 Network switches (Core and Edge Devices)
- .4 Servers and databases
- .5 central management stations
- .6 Network connected system devices and controllers
- .7 Wireless Access Points and wireless controllers
- .8 Mobile phones and tablets
- .9 Any IT System or endpoint connected to the network

1.4. OPERATIONAL TECHNOLOGY (OT) DEVICES AND SYSTEMS

1.4.1. Apply the Cyber security measures listed in the clauses above, in part or in full, as possible, to a wide range of OT Network devices including:

- .1 Industrial Control Systems such as:
 - .1 (PLC's) Programmable Logic Controllers are an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices.
 - .2 (SCADA) Supervisory Control and Data Acquisition is a control system architecture comprising of computers, networked data communications and graphical user interfaces (GUI) for high level process supervisory management.
 - .3 (DCS) Distributed Control System is a computerized control system for a process or plant usually with many control loops, in which autonomous controllers are distributed throughout the system.

- .4 (CNC) Computer numerical Control is the automated control of machining tools (Drills, boring tools, lathes) and 3D printers by means of a computer.
 - .2 Building Management Systems (BMS) and Building Automation Systems (BAS)
 - .3 HVAC equipment
 - .4 Lighting controls for both internal and external applications
 - .5 Energy monitoring and metering equipment
 - .6 Transportation and parking systems
 - .7 Scientific equipment
 - .8 Any other OT System or endpoint that can be connected to the network
- 1.5. REPORT CYBERCRIME
- 1.5.1. Advise the Owner and / or their representatives of any indication of a Cyber Incident of a criminal nature when performing any work on a network connected system.
- 1.6. CYBER SECURITY REPORT LETTER
- 1.6.1. Provide a Cyber Security Report Letter in the closeout documents to the Owner stating which Cyber Security measures have been implemented, when implementing any and / or all of the Cyber Security Measures mentioned in this Specification.

END OF SECTION

28 51 00.00 Intercom System

1. General

1.1. PURPOSE

- 1.1.1. The purpose of the Security Intercom System is to provide fast "duplex," (hands-free at both ends) communication as required to provide instant intercommunications for employees and visitors, emergency paging and signaling, alarm distribution, and audio program distribution. The system assists with personnel safety, facility security, security systems integration, operational efficiency, and maintenance functions.

1.2. SCOPE OF WORK

- 1.2.1. Provide an intercom system as shown on drawings and as specified here in.
1.2.2. Provide an entryphone system as shown on drawings and as specified here in.

1.3. INTERCOM AND ENTRYPHONE SYSTEMS REQUIREMENT

1.3.1. PERFORMANCE REQUIREMENTS

- .1 The Intercom and Entryphone systems shall be IP based.
- .2 The central exchange is connected in such a matter to create a single system. All necessary data, video and audio routing within the systems is via IP or other communicating protocols with the necessary software licenses based on the systems design. No additional proprietary hardware is necessary to do the networking between exchanges
- .3 Ensure systems consists of duplex master stations with direct access buttons, with or without buttons. Each master station calls all other stations within the systems unless specifically blocked or restricted through programming.
- .4 Ensure the master stations are desk, flush or surface wall mounted, or rack mounted as shown on the plans.
- .5 Ensure Substations are flush or surface mounted, tamper and weather resistant where needed and located as required for direct access calling masters.
- .6 Coordinate with the elevator company to install elevator car substations.
- .7 Ensure the systems includes a master control station at or near the central exchange to function as system maintenance and fault indication station.
- .8 Ensure all features and functions is programmed on site with a standard PC via IP and or from master stations.

1.4. INTERCOM SYSTEM FUNCTION REQUIREMENTS

- .1 A designated group of master stations can be called from any door station; any designated master can answer the call.
- .2 A designated group master stations can be called from any substations; any designated master can answer the call. External speaker and emergency call button can also be added.

- .3 A designated group of up to the full capacity of the system with any mix of master stations and door stations can be called from a master station. System needs to be pre-programmed to function.
- .4 Call (Communication) Transfer: A master station can transfer a conversation to any master station within the system.
- .5 Call Forwarding: Incoming calls can be automatically forwarded to another receiving station or telephone. The receiving station number or telephone number can be registered at the original forwarding station. Ensure unit number is assigned to each telephone number.
- .6 Time-Based Call Forwarding: All incoming calls to the original station can be automatically rerouted to a designated master station or telephone number during a specific period of the day.
- .7 No Answer Call Forwarding: Calls to the original station are automatically rerouted to a designated receiving station if the called party does not respond within a pre-set period of time.
- .8 Monitoring: Any door, room or substation can be monitored from a master station. A master station can also disable this function if monitoring is not necessary.
- .9 Scan Monitoring: Any pre-programmed door stations or room sub stations can be scan monitored.

1.5. ENTRYPHONE SYSTEM FUNCTION REQUIREMENTS

- .1 Enable visitors to communicate with residents via mobile application, 2-way audio and, 1-way video calls (visitor/entryphone video to resident's cellular phone and or smart hand held device)
- .2 Enable residents to grant or deny the entry of visitors into the building from land line telephone and or cellular phone and or smart hand held device.

2. Product

2.1. GENERAL

- 2.1.1. Where product model is specified and are deemed discontinued by the product manufacturer, provide the latest manufacturer recommend product model at the time of installation in leu of the specified model.
- 2.1.2. Where product performance specifications are provided, provide the latest manufacturer product model at the time of installation.
- 2.1.3. All products and materials must be new and approved in the pre-installation submittals.
- 2.1.4. Ensure exterior devices are sealed and protected against weather conditions including heat, cold, moisture, dust, and sand.
- 2.1.5. Commercial-grade, high quality, and rated for the environment in which it is being installed
- 2.1.6. Compatible with the intercom system.

2.2. APPROVED SYSTEM

2.2.1. Approved manufacturers

- .1 Intercom: Aiphone or equivalent

- .2 Entryphone: Mircom or equivalent

2.3. MASTER STATION

2.3.1. Manufacturer

- .1 Intercom: Aiphone IX-MV7-HB-L or equivalent
- .2 Entryphone: Desk telephone that is compatible with the entryphone system

2.4. SUBSTATION

2.4.1. Manufacturer

- .1 Intercom: Aiphone IX-DV or equivalent
- .2 Entryphone:
 - .1 Customizable display of various layouts, videos and groups as well as promotional or site specific information.
 - .2 Vandal resistant enclosure
 - .3 Color anti-glare, industrial grade, thick glass touch screen display
 - .4 Minimum 1600 nits high brightness display
 - .5 Touch screen works under any weather condition – rain, snow and when the user is wearing gloves
 - .6 Built-in proximity card reader for easy integration to access control panels
 - .7 Native integration with access control and elevator restriction functionality
 - .8 Recurring revenue opportunities with advertising feature
 - .9 Communications via analog telephone line or SIP for telephone interconnectivity.
 - .10 VOIP and POTs capability
 - .11 Supports mobile application with SIP service for 2-way audio and 1-way video calls
 - .12 Include Auto Dialer functions
 - .13 Full color industrial grade touch screen display that is viewable in direct sunlight
 - .14 Constructed of stainless steel
 - .15 Built-in HD camera and proximity card reader
 - .16 Multi-language support; English and French
 - .17 Configurable themes (color & font), pre-set themes, and screen layout templates
 - .18 Configurable Welcome Screen
 - .19 Built-in keyboard layouts (Full QWERTY, Full QWERTY + Num pad, or Simple)
 - .20 Intuitive call interface using one call button or one-call button per resident
 - .21 Voice or video based help menu for ease of use
 - .22 Elevator restriction
 - .23 Programming via built-in USB and Ethernet ports
 - .24 Remote Desktop capability to fully control programming and setup
 - .25 Load media content via built-in USB interface or remotely via TCP/IP. Supports JPG, GIF, SWF, WMV and MPEG file formats

- .26 Industry Canada and F.C.C. approved
- .27 AODA compliant
- .28 Stainless steel finish
- .29 Mounting: Flush, surface, Pedestal
- .30 Operating Temperature: Outdoor rated for outdoor mounted entryphone and indoor rated for indoor mounted entryphone
- .31 Mircom or equivalent

2.5. RELAYS

- 2.5.1. Provide controllers and or relays to integrate the intercom and entryphone systems with the access control and door release.

- .1 Intercom: Aiphone IXW-MA or equivalent
- .2 Entryphone: Relay that is compatible with the entryphone system

2.6. WIRING

- 2.6.1. Provide all intercom and entryphone systems manufacturer recommended wiring to facilitate a complete turnkey intercom system.

2.7. POWER SUPPLY

- 2.7.1. Provide all intercom and entryphone systems manufacturer recommended power supply to facilitate a complete turnkey intercom system.

2.8. SOFTWARE LICENCE

- 2.8.1. Provide all intercom and entryphone systems manufacturer recommended software licence to facilitate complete turnkey systems.

3. Execution

3.1. INSTALLATION

- 3.1.1. Engage a factory-authorized service representative to supervise and assist with startup service. Complete installation and startup checks in accordance with manufacturer's written instructions.
- 3.1.2. Upon project commencement, Provide qualified technical personnel on-site. Ensure personnel are present on each consecutive working day until the system is fully functional and ready to begin the testing phase of this project.
- 3.1.3. During the installation process maintain an up-to-date set of as-built shop drawings, which is always be available for review by the Owner and/or Engineer's Representatives. This set of documents should be annotated with as-built data as the work is performed. These documents are reviewed as part of the approval process when evaluating payment request applications. At a minimum, the drawings should contain the following information:
 - .1 Quantity and location of all equipment installed.
 - .2 Cable and wire run along with the designation tags assigned to each.
 - .3 Wiring diagrams that indicate terminal strip layout, identification, and terminations.

- 3.1.4. Maintain continuous coordination with the Engineer's Representatives. Ensure the engineers are kept informed of the progress and all conflicts that arise during this project.
- 3.1.5. Provide all proprietary intercom substation back boxes for rough-in.
- 3.1.6. Provide and install all wiring as required.
- 3.1.7. All installation, configuration, setup, program, and related work is performed by technicians thoroughly trained by the manufacturer in the installation and service of the equipment provided.
- 3.1.8. Install all devices and wiring as specified by the intercom system manufacture.
- 3.1.9. Provide and install all intercom control units, add-on control units, and all miscellaneous hardware for a complete turnkey intercom system.
- 3.1.10. Provide and install all master intercom stations and intercom substations as indicated on contract documents.
- 3.1.11. Coordinate with the Owner, configure and program the intercom system as required to suit operations of the facility as directed by the Owner.

END OF SECTION

SUPPLEMENTARY SECURITY BID FORM

FOR

Northern Birch Credit Union Fit-Up
PROJECT: 17488.003.ESS.001

DATE: _____

1. SECURITY TENDER DOCUMENTS

We further confirm that we have received the following documents:

- a) Supplemental Security Bid Form, SUPP SEC. T.F. - 1 to 2.

2. UNIT PRICES

The following prices shall be in effect for the duration of the project. Prices indicated below will be used as a basis for determining pricing if change notices arise during the project. The prices are to include profit, overhead (supervision, financing, administration, parking, mileage, truck fees and related items) but should not include GST. Where a particular product is not offered by the manufacturer enter a value of N.A. (not applicable). **Supply and install all items as per the Specification unless otherwise noted.**

The following information in this section must be completed in order for a Supplementary Tender Submission to be considered complete.

Description	Add	Delete
Refer to specifications and drawing details, provide one Type 1 VSS camera complete with all wiring, mounting brackets, power supplies, and software licence/s.		

Description	Add	Delete
Refer to specifications and drawing details, provide one Type 2 VSS camera complete with all wiring, mounting brackets, power supplies, and software licence/s.		

Description	Add	Delete
Refer to specifications and drawing details, provide one Type 3 VSS camera complete with all wiring, mounting brackets, power supplies, and software licence/s.		

Description	Add	Delete
Refer to specifications and drawing details, provide one Type 4 VSS camera complete with all wiring, mounting brackets, power supplies, and software licence/s.		

Description	Add	Delete
Refer to specifications and drawing details, for a single door located 50 M from controllers; provide one door contact. Provide all wiring and controllers.		

Description	Add	Delete
Refer to specifications and drawing details, for a single door located 50 M from controllers; provide one door contact, one card reader, one motion request to exit device and one electric lock. Provide all wiring and controllers.		

Description	Add	Delete
Refer to specifications and drawing details, for a single door located 50 M from controllers; provide one door contact, two card readers, and one electric lock. Provide all wiring and controllers.		

SUBMITTED BY: _____
(Company)

(Address)

SIGNING OFFICER: _____
(Printed Name)

(Signature)