

1. GENERAL REQUIREMENTS

1.1 INTRODUCTION

- .1 This document provides General Requirements applicable to security related projects undertaken by or on behalf of York Region. These requirements are at all times subordinate to the requirements as defined in the Project Specifications and related documents.
- .2 The *Security Contractor* shall be responsible for the supply, installation, configuration, testing and commissioning of the fully operational *ACAMS* to the satisfaction of the Region, or designate.
- .3 The General Contractor shall only use one of the Region's pre-approved *installers* to perform the installation of the *ACAMS*, including supply of cabling; see [Appendix A: Prequalified Security System Vendors](#).
- .4 The General Contractor shall only use one of the Region's pre-approved *Integrators* to program a Lenel *ACAMS* and to supply hardware, equipment, and licencing of a Lenel *ACAMS*; see [Appendix A: Prequalified Security System Vendors](#).
- .5 The General Contractor shall only use Honeywell Building Automation to program a Honeywell *ACAMS* and to supply hardware, equipment, and licencing of a Honeywell *ACAMS*; see [Appendix A: Prequalified Security System Vendors](#).

1.2 ABBREVIATIONS

- .1 *ACAMS* Access Control and Monitoring System, see definitions
- .2 *ACS* Access Control System
- .3 *ADO* Automatic Door Operator
- .4 *CR* Card Reader
- .5 *CS* York Region Corporate Security Team
- .6 *DC* Door Contact
- .7 *IDS* Intrusion Detection System, see definitions
- .8 *IP* Internet Protocol
- .9 *ITS* York Region Information Technology Services Team
- .10 *LAN* Local Area Network
- .11 *MAG* Electromagnetic Lock
- .12 *NEMA* National Electrical Manufacturers Association
- .13 *POE* Power Over Ethernet
- .14 *PTZ* Pan, Tilt and Zoom Camera
- .15 *REX* Request to Exit Sensor, see definitions
- .16 *RFA* Request for Assistance, see definitions
- .17 *SCADA* Supervisory Control And Data Acquisition, see definitions
- .18 *TLS* Transport Layer Security Protocol
- .19 *UPS* Uninterruptible Power Supply, see definitions
- .20 *VMS* Video Management System
- .21 *WAN* Wide Area Network, see definitions

1.3 DEFINITIONS

- .1 *ACAMS*: integrated security system including an *ACS*, *IDS* and *VMS*.
- .2 *Access Level*: customizable set of permissions granted to a user or group to access secure spaces or perform specific actions. Permissions may be further customized using schedules.
- .3 *Alarm*: is a status in the *ACS* or *IDS* when a situation occurs which requires immediate on-site investigation.
- .4 *Alert*: a notification from the *ACAMS* to notify of unusual conditions. Alerts may escalate to alarms if the situation worsens.
- .5 *Arming Station*: consists of an arming button, arming *CR* and keypad. Used for local arming of *IDS*.
- .6 *Bond Sensor*: device used to measure the force required to hold an object in place or the force exerted by an object when held. Used to ensure that a *MAG* maintains the necessary force to properly secure doors.

- .7 *Explosion Proof*: refers to the certification required of electrical and related safety devices used in hazardous locations.
- .8 *Fail Safe*: system or mechanism designed to automatically default to an open or unlocked condition in the event of a failure or malfunction.
- .9 *Fail Secure*: system or mechanism designed to maintain security by remaining locked or secure in the event of a failure or power loss.
- .10 *Forced Entry*: An alarm that is generated on the ACS when a door monitored by the ACS is opened without prior authorization from the ACS.
- .11 *Hold Open*: An alarm that is generated on the ACS when a door monitored by the ACS remains open for an extended duration after an authorized opening.
- .12 *IDS*: is a system to monitor, detect and notify unauthorised access or the deviation of sensor observations from acceptable values.
- .13 *Integrator*: is a pre-qualified contractor responsible for programming and supplying hardware, equipment, and licences for the ACAMS.
- .14 *Installer*: is a pre-qualified contractor responsible for installing the ACAMS and its components.
- .15 *Intrusion Alarm*: An alarm generated by the IDS immediately after any *intrusion zone* faults while the IDS is fully armed.
- .16 *Intrusion Zone*: area monitored by the IDS with 1 or more DC and/or glass break sensors
- .17 *RFA button*: security device designed to be activated quickly and easily by staff in emergency situations to notify appropriate personnel. Device may be wired or wireless.
- .18 *RFA*: an alarm triggered by activation of a *RFA button* or Universal Washroom Emergency Call button.
- .19 *REX*: a component in the ACAMS that allows individuals to exit a secured area without triggering an alarm or compromising security protocols.
- .20 *Security Contractor*: is inclusive of both the *integrator* and *installer*
- .21 *Supervision*: refers to the continuous monitoring and self-checking of the system's components to ensure they are functioning correctly and are not compromised.
- .22 *SCADA*: is a system used for monitoring and controlling industrial processes and infrastructure, gathering real-time data from remote locations.
- .23 *UPS*: is a device that provides backup power to electrical equipment in the event of a power outage or fluctuation, ensuring continuous operation and protection against data loss or hardware damage.
- .24 *Valid Card Swipe*: Presentation of proximity card or tag to a CR and subsequent authentication of user *Access Level* by the ACS.
- .25 *WAN*: is York Region's telecommunications network that extends throughout the Region, connecting multiple smaller networks at remote sites, such as *LANs*, to facilitate communication and data exchange across the Region.

1.4 ACAMS OPERATION - GENERAL

- .1 The ACAMS automatically uploads/downloads information to/from the control panels while the control panels are in communication with the central server. Data transfer does not interfere with normal operations.
- .2 User Interface
 - a. Graphical interface has a multilayer hierarchy where the highest level is a map of York Region showing each connected facility on the map using appropriate icon based on the facility designation (eg: corporate, environmental, paramedic).
 - b. Each connected facility has a dedicated graphical display or series of displays. Dedicated facility graphics:
 - i. are based on applicable architectural floor plan for that facility;
 - ii. include the current real-time status of the Facility and all field devices, including cameras, RFA buttons, strobes and remote release buttons;
 - iii. allow direct control of system functions at the site, such as arming, disarming, and door control; and
 - iv. Show the AC power status using the facility's main panel power fail input to monitor AC power status.
- .3 Audit Trail / Event Log

- a. The central server maintains a consolidated event log for every connected site within the Region's portfolio.
 - b. Event Log includes:
 - i. All access card activities including name, and action granted or denied
 - ii. Logging in and out of operators
 - iii. Scheduled activations and deactivations
 - iv. Trouble and alarm reports
 - v. All failures, arming and disarming of systems
 - vi. System resets and restarts
 - vii. Intrusion detection alarms
 - viii. All system events on the IDS
 - ix. For elevators on ACS, all card swipes and subsequent button presses for floor(s) selected / elevator call.
 - x. For parking controls on ACS, the parking control open/close status information.
 - c. The local system at each site holds at least 24 hours or 5,000 events in a rolling log. New records overwrite the oldest records once the log capacity is reached.
 - d. Upon loss of communication with central server, alarms continue to sound locally, and events continue to be recorded in the local event log. Once communication is restored, these records are automatically transferred to, and saved on, the consolidated event log on the central server.
- .4 Third Party Monitoring
- a. Each *IDS* panel has at least 2 paths of communication to the 3rd party monitoring service including hard-wire *LAN* and cellular.
 - b. All arming and disarming events are communicated to the 3rd party monitoring service.
 - c. All *alarms* are communicated to the 3rd party monitoring service.
 - d. *Alerts* are not communicated to the 3rd party monitoring service.
 - e. Each *IDS* panel sends receiver supervision time signals to the 3rd party monitoring service following the 1 hour NFPA 72 standard.
 - f. *IDS* reports power loss to 3rd party monitoring service.
- .5 ACS
- a. Authentication on the *ACS* is based on *access levels*. *Access levels* are managed by *CS*.
 - b. Upon *valid card swipe*, at a pedestrian door, the *ACS* authorizes entry and temporarily releases the electric locking device allowing the door to be opened.
 - c. Upon *valid card swipe*, at a vehicle entry point (gate or door), the *ACS* authorizes entry and commands the entry point to automatically open temporarily.
- .6 Arming and Disarming of *IDS*
- a. Arming at each Facility only occurs when the system is Ready to Arm, as indicated on the *IDS* keypad. This arming process may proceed if *alerts* are present.
 - b. Local arming is triggered following a *valid card swipe* on a dedicated arming *CR*, followed by a press of the dedicated arming button. System then fully arms after exit delay of 45 seconds.
 - c. *IDS* automatically disarms, upon an authorized entry to the facility. The door does not have to be opened for the *alarm* system to be disarmed.
 - d. *IDS* can also be armed and disarmed remotely (either manually or automatically) via the central server.
 - e. Arming *CR* cannot be used to disarm *IDS*.
- .7 Alarms and Alerts
- a. Each door controlled by the *ACS* generates *forced entry* and *hold open alarms*.
 - i. A forced entry alarm is generated when a *forced entry* occurs.
 - ii. Manual key entry to a facility is treated as a *forced entry*.
 - iii. A *forced entry* is not generated, if the *REX* associated with the door is triggered or activated prior to the door opening.

- iv. An *alert* is generated if a door remains open for 45 seconds following an authorized entry/exit from a secured space.
 - v. A *hold open* is generated if a door, without *ADO*, remains open for 10 seconds following an *alert* from that door. Integral beeper on the CRs associated with the held open door will sound and continue to sound until the door is closed.
 - vi. A *hold open* is generated if a door, with *ADO*, remains open for 10 seconds beyond the *ADO* cycle time following an authorized entry/exit from/to a secured space. Integral beeper on the CRs associated with the held open door will sound and continue to sound until the door is closed.
 - vii. *Forced entry* and *hold open alarms* on doors for Corporate and SCADA data centres are treated as *intrusion alarms*.
 - b. *ACAMS* signals a “tamper trouble” *alert* when any supervised wires are cut or short circuited.
 - c. *Intrusion Alarms* are only triggered when the *IDS* is fully armed.
 - d. All *intrusion alarms* are annunciated:
 - i. Locally on all keypad(s) at the Facility;
 - ii. On the *ACS* Alarm Monitor application;
 - iii. To the 3rd party monitoring station; and
 - iv. To the *SCADA* system, where applicable.
- .8 *IDS* Keypads
- a. Display the name of the facility and the nature of any faults in the system.
 - b. Are not used for Arming, Disarming, or clearing of any faults.
 - c. Indicate ‘Ready to Arm’ while the *IDS* is disarmed and all intrusion points are “fault free”
 - d. During the “Exit Delay” after initiating arming sequence, sounders beep slowly and display shows “Exit Delay in Progress”
 - e. When the *IDS* is fully armed, sounders are silent and the “armed” status indicator is illuminated.
- .9 *VMS*
- a. Camera stream recordings are stored on remote recording servers via the *WAN*.
 - b. Camera streams record at different frame rates depending on if there is motion in the field of view.
 - c. Video recordings include a burn in of the date, time and the camera description on every frame of the recording.
 - d. Privacy Masks are added:
 - i. For staff spaces, directly above the staff member’s chair, to cover the person however leaving hand activity visible.
 - ii. For resident room doorways in long term care facilities, to cover the door.
 - iii. For exterior cameras that capture public’s homes, to cover the public’s entire homes
 - iv. For holding cells, to cover the toilets.
 - v. For safes, to cover the code entry keypad
 - vi. As directed by *CS*
 - e. Following a loss and subsequent restoration of communication between camera and server, local recordings of cameras with local storage, are uploaded to the remote recording server to recover any gaps in recording coverage.
- .10 Intercom Systems

- a. When activated, the remote intercom initially calls an associated intercom master station, where provisioned, and, if unanswered or not provisioned, routes the call to a designated phone number.
- b. When the remote intercom is activated, video from the intercom is recorded on *VMS*.
- .11 *RFA*
 - a. *RFA* is triggered any time an *RFA button* or Emergency Call Button in a washroom is activated.
 - b. *RFA* remains active until the *alarm* is acknowledged using the 'panic all clear' button on the associated graphic.
 - c. When a *RFA* is triggered, the graphic map on the *ACS* shows the exact location of the *RFA button* (either actual or assigned) and a description of the *alarm*.
 - d. When a *RFA* is triggered, the associated strobes light and piezo buzzers sound.
 - e. Strobes in security offices are associated with all panic buttons in the facility
 - f. Strobes in employee only program spaces are associated with the *RFA buttons* in the facility associated with that program area.
 - g. Strobes outside designated rooms are only associated with *RFA buttons* within the room.
 - h. Wireless *RFA buttons* are each assigned to a specific room.
- .12 Universal Washroom
 - a. Each Emergency Call Button is connected to both *ACS* and *IDS* for monitoring.
 - b. Activation of Emergency Call Button triggers an *RFA* on the *ACS* graphic and *IDS*.
- .13 Lockdown Button
 - a. When a Lockdown button is activated, schedules are ignored, and all associated doors default to locked state and are only accessible by *valid card swipe*.
 - b. When the Lockdown button is deactivated, all associated door schedules resume normal operation.
- .14 Glass Break Sensor
 - a. Glass break sensors trigger an *alarm* on the *ACS* whenever the sensor is triggered.
 - b. When an *alarm* is generated on the *ACS* from a glass break sensor, the graphic map shows the exact location of the sensor and a description of the *alarm*.
 - c. *Alarms* from glass break sensors on the *ACS* remain active until the alarm is acknowledged using the 'glass break all clear' button on the associated graphic.
 - d. Glass break sensors trigger an *Intrusion Alarm* on the *IDS* only if the sensor is triggered while the system is fully armed.
- .15 *REX*
 - a. Motion *REX*
 - i. Motion *REX* are configured to shunt *forced entry* only; triggering of a motion *REX* does not release the electric door strike.
 - b. Exit Button *REX*
 - i. Activation of Exit Button *REX* temporarily releases associated *MAG*, activates secure side *ADO* activation device, where present, and allows associated door to be opened.
- .16 Remote Release button
 - a. Activation of a remote release button associated with an automatic gate or overhead door causes the portal to temporarily open automatically.
 - b. Activation of a remote release button on a door without *ADO*, temporarily releases the electric locking device. The door can then be opened manually.
 - c. Activation of a remote release button on a door with *ADO*, temporarily releases the electric locking device, and temporarily activates the non-secure activation device. The door can temporarily be opened manually or automatically, by triggering the non-secure side activation device to activate the *ADO*.
- .17 *MAG*
 - a. The Bond sensor reports if the corresponding door is improperly closed.
 - b. Where installed on a double door, both doors are treated as a single opening.
 - c. Upon power loss to the magnet, the Bond sensor reports the door as *forced open* irrespective of whether the door opened.

.18 ADO

- a. For all ADOs installed on doors with ACS Control:
 - i. CR on the insecure side of the door is always active.
 - ii. ADO activation device on non-secure side of the door is inactive, except following a *valid card swipe* on associated CR, activation of associated remote release button or if door is unlocked by schedule.
 - iii. The door is normally closed and locked unless scheduled otherwise.
 - iv. If there is no maglock on the door, the ADO activation device on the secure side of the door is always active.
 - v. If there is a maglock on the door, the ADO activation device on the secure side of the door is normally inactive.
- b. When a person is entering a secure space via a door with ADO installed:
 - i. Upon valid card swipe, non-secure side activation device is temporarily activated, and the electric locking device released.
 - ii. The door can then be opened manually or automatically, by triggering the non-secure side activation device to activate the ADO.
 - iii. After opening or time delay, the door will relock, and the non-secure side activation device will become inactive.
- c. When a person is leaving a secure space via door with ADO installed:
 - i. Door without MAG: The door can be opened manually or automatically, by triggering the secure side activation device to activate the ADO. The door relocks after opening.
 - ii. Door with MAG: The secure side activation device is normally inactive. Exit button REX activation is required to release MAG and activate the secure side activation device. After Exit button REX activation, the door can temporarily be opened manually or automatically, by triggering the secure side activation device to activate the ADO. The door relocks after opening or time delay and the secure side activation device becomes inactive.
 - iii. Motion REX, if present, is integrated with ADO activation device.

.19 Elevator Access Control Integration

- a. Where a CR is installed in an elevator cab, upon *valid card swipe*, the floor buttons corresponding to authorized floors are temporarily unlocked in that elevator cab only, for the user to select.
- b. Where a CR is installed in an elevator lobby, upon *valid card swipe*, the elevator is called to that lobby.
- c. The ACS does not affect the service, or fire mode operation of the elevator.
- d. If the CR loses communication with the controller, floors remain in fail secure condition.
- e. ACAMS does not monitor or capture elevator operational alarms.
- f. Each elevator with ACS control has a toggle switch (or key switch) to bypass ACS. In bypass mode, the elevator operates as if there was no ACS.

.20 Parking Controls

- a. ACS Integration
 - i. All control functions for barrier operation are controlled through the ACS.
- b. Parking Operator
 - i. Entrance barrier opens automatically via signal from the ACS upon *valid card swipe* at either CR on the access control pedestal or via ultra long-range CR (where present).
 - ii. Entrance barriers may also be opened remotely through the ACS graphical interface, intercom system or, where present, by remote release button.
 - iii. Parking controls at an exit open on vehicle departure when the departure loop senses the vehicle.
 - iv. Barriers reclose when the associated reset loop detects the vehicle passing beyond the barrier or timer elapses.
 - v. Parking control loops do not function in reverse.
- c. Barrier Arm

- i. If a barrier arm encounters an object while closing, the barrier arm immediately signals an *alarm* to the ACS and completely opens.
 - ii. Barrier arm can be manually operated locally in the event of a power or communications failure.
- .21 Monitor Points
 - a. Main Incoming Power Status
 - i. Monitor main incoming 120VAC supply to ACS and reflect status on site graphic.
 - b. Generator Run Status
 - i. Monitor generator run status on ACS and reflect run status on site graphic.
 - c. Vaccine Fridges and Freezers Alarm
 - i. Monitor the alarm point on ACS and IDS and reflect alarm status on site graphic.
 - ii. *Alarms* are triggered and communicated to the 3rd party monitoring station irrespective of the arming status of the IDS.

1.5 SECURITY SYSTEM SUBMITTALS

- .1 General
 - a. All submittals shall be provided in electronic format. Submittals shall be provided in PDF, without electronic locks, encryption, or restrictions. Drawings shall also be provided in AutoCAD (DWG) format.
 - b. All submittals must adhere to the Region defined naming convention (see [Appendix B: Security System Naming Convention Standards](#)) for all system components and must be consistent with the names used in the software and on site.
 - c. Submittals shall include at least the following:
 - i. System riser diagram(s)
 - ii. System layout/floorplan
 - iii. Network connectivity diagrams
 - iv. Vertical and horizontal wiring diagrams
 - v. Site Specific point-to-point wiring diagrams and schematics
 - vi. Device landing schedule(s)
 - vii. System integration schematic(s) and wiring diagrams
 - viii. Tub/enclosure layout diagram(s)
 - ix. 120 VAC Line Voltage Electrical connections and wiring diagrams
 - x. Addressing and dip switch setting charts
 - xi. Product specifications and cut-sheets
 - xii. Complete Bill of Materials
- .2 Shop Drawings
 - a. The *integrator* shall produce the complete set of shop drawings for approval by CS or designate.
 - b. The security contractor shall NOT start any implementation work until the shop drawings are approved.
 - c. Shop drawings shall cover the entire scope of the Work and shall include all submittal items identified under [1.5.1 General](#) and also the following:
 - i. Any dependencies which are not included in these Drawings, such as wall space, electrical requirements, and air conditioning.
 - ii. Any compatibility issues between the existing installation and the proposed new equipment.
- .3 As-Built Documentation
 - a. The as-built documentation for the ACAMS installation shall be submitted for approval by CS or designate, as a requirement to achieve substantial performance of the Work.
 - b. As-built documentation shall cover the entire scope of the Work that was completed under the Contract Documents, and shall include all submittal items identified under [1.5.1 General](#) and also the following:

- i. All technical notes, software scripts, firmware details and other documentation covering the IT portion of the Work covered under this Contract.
 - ii. IDS configuration files
 - iii. List of serial numbers for all supplied parts
 - iv. List of IP and MAC addresses for networked devices
 - v. Lists of all usernames and passwords used for the installation and configuration of the system and devices
 - vi. Splice box locations marked on the wiring diagram
 - vii. Commissioning documentation (see [Appendix C: Security System Commissioning Forms](#)). The commissioning documentation must be completed by the *integrator* and signed by the Consultant, if applicable, and Regional representative.
- c. Hard copy of approved documents shall be included inside main security enclosure.

1.6 TESTING AND QUALITY ASSURANCE

- .1 ITS Software and Hardware Penetration Testing
 - a. The *integrator* shall work with ITS to perform security penetration testing for supplied hardware and/or software, as required by ITS.
 - b. The *integrator* shall supply, if requested, copies of all network device specifications and data sheets to ITS in preparation for the penetration testing.
 - c. The *integrator* shall supply, if requested, a demo of each device type to ITS for penetration testing.
- .2 Site Testing
 - a. Site testing shall be performed by the *integrator* following installation of, or modification to, the ACAMS at a facility.
 - b. During site testing, the *integrator* shall complete the Region's commissioning forms (see [Appendix C: Security System Commissioning Forms](#)) to confirm that all hardware and software components of the system are installed and functioning as intended.
 - c. Following successful testing (i.e. no remaining failed tests), the *integrator* shall submit completed forms to Region, or designate.
- .3 Commissioning
 - a. After site testing has been completed, commissioning shall be scheduled with the Consultant, if applicable, and Regional representative(s).
 - b. The *integrator* shall demonstrate, to the satisfaction of CS, that the system and all of its components are functioning, as per the contract documents. This approval process shall be performed in 2 phases:
 - i. A virtual commissioning with the Region's Security System Administrator
 - ii. A final in-person commissioning with CS.
 - c. All failed tests shall be corrected, and retested until successful test is achieved, prior to the Consultant approving, and the Region accepting the system.

1.7 WARRANTY & TECHNICAL SUPPORT

- .1 The Security Contractor shall provide all warranty services for ACAMS for a period of twenty-four (24) months from the date of Total Performance of the Work and shall provide all necessary material required to replace any defective products during this period.
- .2 The beneficiary of the Warranty shall be the Regional Municipality of York.
- .3 The *integrator* shall always have qualified technical support available during normal working hours and emergency support available throughout the warranty period.

1.8 CLOSE OUT

- .1 Project Close Out process requires that the following documents and miscellaneous items are completed and provided to the Region:

- a. Assignment of all warranties, licences and product registrations to the “Regional Municipality of York” and documentation to this effect;
- b. All associated work is reported to, and permits are closed out with, appropriate Authority Having Jurisdiction;
- c. Ensure that all temporary configurations are returned to their permanent “operational” status and appropriate documentation is provided confirming this status;
- d. All installation software, accessory cables, calibration units and any other material accompanying the installed equipment; and
- E. All keys, special tools, spare parts, unused components, permits, approvals, as-built documentation and project related documentation.

1.9 NETWORK TCP/IP COORDINATION

- .1 Configuration and activation of *LAN* equipment maintained by *ITS* is to be co-ordinated by the Region. The *integrator* shall provide two weeks advance notification to the Region for configuration of network ports.
- .2 IP addresses shall be provided by *ITS* on request from the *integrator* to the Region.
- .3 Communications between all distributed security devices on the *WAN* shall use TCP/IP protocol. Communications between the security devices that does not involve the Region’s network may use any appropriate protocol.

2. PRODUCTS

2.1 GENERAL

- .1 The *security contractor* is responsible to supply all equipment identified in the contract documents, unless otherwise noted.
- .2 The *security contractor* shall supply all necessary wiring, termination equipment/devices and other necessary miscellaneous components which are not specified in the Contract Documents, but which are necessary to implement a fully functional, and networked, *ACAMS*.
- .3 The *Installer* shall provide new wiring for all new and reused security devices.
- .4 The *Installer* shall provide wire and cable according to the drawings and *ACAMS* requirements; see [Appendix D: Cabling](#).
- .5 The *integrator* shall review the versions of software, firmware and hardware currently in service and validate the compatibility of new installations with the existing system.
- .6 The *integrator* shall supply and install all necessary software licencing to operate the security solution based on the Contract Documents, including integration, camera and CR licenses.

2.2 REGIONAL SECURITY SYSTEM INTEGRATED PLATFORMS

- .1 The Region has 2 *ACAMS* platforms, Lenel and Honeywell
- .2 The Region’s Lenel *ACAMS* is constituted by the following systems:
 - i. ACS is Lenel OnGuard.
 - ii. IDS is Bosch RPS
 - iii. VMS is Lenel Milestone XProtect® Expert.
- .3 The Region’s Honeywell *ACAMS* is constituted by the following systems:
 - i. ACS is Honeywell Enterprise Buildings Integrator.
 - ii. IDS is Honeywell Vista
 - iii. VMS is Honeywell Digital Video Manager.

2.3 NETWORK EQUIPMENT

- .1 All servers and network switches connected to the *LAN* or *WAN* shall be provided by the Region.

2.4 SECURITY SYSTEM DEVICES

- .1 Pre-approved devices and solutions shall be used wherever possible; see [Appendix E - Pre-approved security devices](#).
- .2 The use of any equipment which is not approved by the Region, or designate, is strictly prohibited.
- .3 All *ADO* sequencing boards and electric strikes for doors controlled by *ACS* shall be supplied by the *integrator*.
- .4 All security devices supplied under this contract shall meet the environmental requirements as identified in [Appendix F - Environmental Requirements](#).
- .5 Power supplies shall be provided from a single manufacturer, who must be approved by the security system manufacturer.
- .6 Each *MAG* shall:
 - a. be Plate Magnet style with a minimum holding force of 540 kg.
 - b. have indicator LED's showing if they are closed or open
 - c. have integral hold force sensors (Bond sensor)
 - d. have integral double pole door contacts.
 - e. where installed on a double door, be equipped with separate magnet and plate for each door and enclosed in a single housing.
- .7 *RFA* Strobes shall be blue in colour.

3. EXECUTION

3.1 GENERAL

- .1 The *security contractor* is responsible to install all equipment identified in the contract documents, unless otherwise noted.
- .2 The *security contractor* shall identify and report all pre-existing or related construction defects which will affect the progress of the Work to the Region and the Consultant, if applicable, before commencing construction work.
- .3 The *installer* shall install and wire all *ACAMS* equipment according to the manufacturer's recommendations. Any instances where *installer* fails to follow manufacturer's recommendations shall be corrected by *installer* with no additional cost to the Region.
- .4 Redundant *ACAMS* components and cabling shall be completely removed.
- .5 The security contractor shall limit switchover time to one day when replacing existing *ACAMS* or components, minimizing *ACAMS* down time for the facility. No facility shall remain unsecured overnight.
- .6 Modification of the fire alarm system, and signage is included in the scope of work.
 - a. The *integrator* shall retain appropriate fire company, typically the Region's Fire Alarm System contractor of record for that location, to complete fire system tie-in and testing.
- .7 Permits
 - a. The *integrator* is responsible for permits, and associated coordination (including approvals and inspections, engineered drawings and fire alarm interconnections) associated with *MAG* installation.
 - b. *CS*, or designate, shall be present for final permit inspection for *MAG* installation.
 - c. Electrical permits are not required for retrofit security projects; *security contractor* may report electrical installation work through the Region's Continuous Safety Services (CSS) Program with the Electrical Safety Authority at no cost to the contractor.
- .8 Work at Regional Water and Wastewater facilities
 - a. All work undertaken in hazardous locations shall be coordinated and scheduled with the Region in advance of the work, to have a Regional representative present during the work.
 - b. The Security Contractor shall contact the Region's Remote Operations Centre daily at 905-895-2143 or 905-895-2144 prior to entering or performing any work at the facility.

3.2 SOFTWARE/SYSTEM CONFIGURATION

- .1 The *integrator* shall ensure that the new/updated ACAMS under this contract is configured to follow the requirements outlined in [Section 1.4 - SECURITY SYSTEM OPERATION - GENERAL](#)
- .2 All programming and configurations of the ACAMS completed under this Contract shall be consistent with existing programming.
- .3 All security related work under this Contract shall be reflected in the ACAMS database and associated graphics.
- .4 The *integrator* shall provide their own cellular connectivity to connect to the Region's network for any work under this Contract.
- .5 The *integrator* shall use client applications on a Region provided virtual machine to program, configure and test the system.
- .6 Naming of ACAMS and components
 - a. All system components shall be configured and named as outlined in [Appendix B: Regional Security System Naming Convention Standards](#).
 - b. Component naming shall be consistent throughout the system.
 - c. All alarm points shall have a unique and unambiguous name;
 - d. Name camera with patch panel information in software.
- .7 User Interface
 - a. The *integrator* shall use the existing dynamic icons, approved by CS, to populate the graphical interface or, if necessary, create additional custom dynamic icons.
 - b. The *integrator* shall create custom alarms for each facility which shall clearly display any intrusion and/or alarm events using the ACS Alarm Monitor application.
 - c. The *integrator* shall follow the standard graphic template, at resolution 1920x1080, for facility graphics for Lenel ACAMS (See [Appendix G – Sample Graphics](#))
 - d. The *integrator* shall create hover messages for each item added to the graphical interface.
- .8 Monitor Zones
 - a. The *integrator* shall update existing or, if necessary, create new monitor zones.
 - b. Each facility shall be assigned a single unique monitor zone.
 - c. Each facility monitor zone shall be added to the master monitor zone for the Region.
- .9 The *integrator* to create/update master *access level* for the site which includes all CRs at the site.
- .10 The *integrator* shall update all system hardware components, including cameras, with the latest manufacturer approved firmware versions prior to final commissioning.
- .11 The *integrator* shall change all camera passwords from their factory defaults to a password provided by the Region.
- .12 Server Software and configuration
 - a. The *integrator* will not be provided with direct access to database servers.
 - b. The *integrator* shall work with ITS to perform application or database server programming and configuration.
 - c. All work requiring access to the database and/or application servers must be coordinated with the Region a minimum of one week in advance.
 - d. All changes to the network configuration and network attached devices must be approved by ITS.
- .13 Cameras
 - a. Configure camera settings as provided by ITS and as per [Appendix H: Camera Settings](#).

3.3 INSTALLATION - ELECTRICAL

- .1 The General Contractor's Electricians are responsible to supply and install all new electrical raceways and junction boxes for ACAMS installation. Existing raceways may be reused.
- .2 Install exposed raceways parallel or perpendicular to building lines and group neatly.
- .3 Seal around all conduit penetrations.

- .4 Where emergency power is available at a site, the *installer* shall use dedicated 120VAC emergency circuits for ACAMS installation.
- .5 Where emergency power is not available at a site, *installer* shall use dedicated 120VAC circuits for ACAMS installation.
- .6 Electricians shall not work on “hot circuits” without special permission from the Region.
- .7 Install circuit breaker lockout, in energized position, on each circuit breaker serving the ACAMS

3.4 INSTALLATION – WIRES AND CABLES

- .1 *Installer* is responsible to install cable for ACAMS installation.
- .2 Label all wiring infrastructure, including fibre optic cabling, with wire markers in accordance with [Appendix I: Security System Labelling Requirements](#).
- .3 Cabling in open areas shall be run within raceways.
- .4 Where raceways are available, install cables in raceway.
- .5 Exposed cabling is only allowed above drop ceilings or where otherwise approved by CS.
- .6 Install exposed cables parallel or perpendicular to building lines and group neatly.
- .7 Arrange cables in parallel rows on cable trays.
- .8 Install through-wiring in junction boxes and pull boxes leaving a minimum of 300 mm of slack inside box.
- .9 Install cables in electrical boxes and equipment enclosures located in outdoor, wet or sprinklered areas with watertight cable connectors.
- .10 Use direct burial rated cable for all outdoor applications.
- .11 Where security low voltage wiring is run in parallel to ≥ 110 VAC electrical wiring or conduit, provide minimum of 300 mm separation between the wires.
- .12 Cable Splicing
 - a. All cable runs should be continuous and splice-free.
 - b. If splices are required, approval from CS is required for each splice.
 - c. Each approved splice or junction must be identified and accessible after project completion.
 - d. Splices shall be made in junction boxes utilizing DIN rail-mounted terminal blocks.
- .13 Field device cabling
 - a. For Regional Water and Wastewater facilities shall be home run to security control panel in designated IT room.
 - b. For access control at small facilities (with <10 doors on ACS) shall be home run to security control panel in designated IT room.
 - c. For access control at large facilities (with ≥ 10 doors on ACS) shall be run to local control enclosures.

3.5 INSTALLATION – SECURITY SYSTEM DEVICES

- .1 Label every serviceable component of the ACAMS in accordance with [Appendix I: Security System Labelling Requirements](#).
- .2 All exterior mounted ACAMS components shall be appropriately sealed to prevent intrusion by water or pests.
- .3 A minimum quantity of 10% of inputs, 10% of relay outputs and 10% of CR ports are to remain available for use in all systems which are being affected by the project.
- .4 The location of equipment shown on the Drawings may be revised during construction, but prior to its installation, and the Security Contractor shall not be entitled to any additional costs for the relocation of equipment if the new location is within 1000 mm of the original location.
- .5 All removed equipment shall be immediately delivered to CS upon removal. The Security Contractor to dispose of equipment that CS determines is not required for Region to retain.
- .6 All temporarily removed equipment shall be immediately delivered to CS for temporary storage.
- .7 All surplus equipment shall be delivered to CS upon contract completion.
- .8 Install snubbing diodes in all security devices incorporating electro-magnetic operation including electric strikes and MAGs.

- .9 Install all power supplies and transformers with a back plate and use a common ground wire.
- .10 Electric locks shall be powered from dedicated and independently fused 24VDC power supplies
- .11 All access control board power to be on dedicated 12VDC power supplies
- .12 Install a relay on main incoming 120VAC supply to ACS; connect relay contact to power fail input on the ACS main panel.
- .13 Enclosures
 - a. All control panels and modules shall be housed in enclosures.
 - b. Each enclosure containing a control panel and/or module shall:
 - i. Be wall mounted and located as shown on the drawings.
 - ii. Have key operated lock on the cabinet door, keyed to the Region's designated keyway;
 - iii. Have a monitored cabinet tamper mechanically mounted on the cabinet door;
 - iv. Have NEMA rating suitable for the installed environment, as identified in the contract documents; and
 - v. Be sized sufficiently to ensure ease of maintenance, adequate ventilation, and space for 20% expansion
 - c. Each enclosure containing one or more ACAMS control panels shall:
 - i. Include power back-up from a smart UPS (with network and power monitoring software functionality);
 - ii. Include a dedicated network jack for maintenance purposes;
 - iii. Have residential style light switch for local power disconnect inside the enclosure
 - iv. Have a switched LED light inside panel, upstream of local power disconnect, for Water and Wastewater facilities only; and
 - v. Be fed from dedicated 120VAC power circuit.
 - d. Cabinets containing local door control modules shall be installed on secure side, in vicinity to the door and at most, 2500 mm above the floor.
 - e. If enclosure is installed above finished drywall ceiling, access hatch shall be installed for servicing.
- .14 Supervision
 - a. Install supervision on all *DC* and *REX* connected to *ACS* at the remote end of the detection line using 2 resistors to provide 4 state monitoring.
 - b. Install supervision on each field device monitored by the *IDS* at the remote end of the detection line using 1 resistor to provide 2 state monitoring.
- .15 Third Party Monitoring
 - a. The *integrator* shall program and test the *IDS* connection, along each communication path, to the 3rd party monitoring.
 - b. The *integrator* shall coordinate configuration and testing of the system for each relevant signal with the Region's 3rd party monitoring service.
 - c. Cellular antenna shall be installed appropriately to ensure a consistent and reliable signal. Minimum acceptable signal strength is 'good'.
- .16 *RFA*
 - a. Hard-wired *RFA buttons* connected to fixed furniture shall be located facing away from the user and in a discreet location, but easily accessible to the employee.
 - b. Hard-wired *RFA buttons* in first aid rooms shall be located near the bed and clearly identified.
 - c. Piezo buzzers shall be located in the ceiling space, in proximity to its associated strobe.
- .17 *CR*
 - a. All conductors in *CR* cables shall be connected both at the *CR* and its associated control board reader port as per the following layout:
 - Red – 12VDC
 - Black – Ground (RTN)
 - White – Wiegand Data 1 / Clock / RS485-A
 - Green – Wiegand Data 0 / Data / RS485-B
 - Orange – LED Input (Green)

Yellow – Beeper Input
Blue – Hold Input / LED Input (Blue)
Brown – LED Input (Red)
Bare – Drain

.18 MAG

- a. Where possible, *installer* shall install *MAG* on secure side of door.
- b. For all interior doors, connect the *Bond Sensor* to the *ACS* only.
- c. For all perimeter doors, connect the *Bond Sensor* to the *ACS* and *IDS*.
- d. Integration of exit button with *MAG* shall be with physical wiring only.

.19 DC

- a. *DC* associated with doors controlled by *ACS* shall be directly connected to *ACS*.
- b. *DC* associated with perimeter access doors, exterior hatches, and data centres shall be directly connected to *IDS*.
- c. *DC* installed on a hollow door with trough to be secured with silicone.
- d. *DC* installed on an overhead door to be installed at height specified in door detail drawing.

.20 ADO

- a. *ADO* is typically supplied and installed by others.
- b. Install door interface relay on each *ADO* with *ACS* control to integrate the *ADO* operation with the *ACS*.
- c. Door interface relay shall be powered via power supply for *ACS* and not *ADO*.

.21 REX

- a. Locate motion *REX* on secure side of door so that the sensor is triggered by all individuals exiting through the door.
- b. *REX* associated with door that has *DC* or *MAG* connected to *IDS* shall also be connected to *IDS*.

.22 Electric Strikes

- a. Shall be configured to fail secure.
- b. Install in-line power controller for each electric strike.
- c. Install appropriate face plate for electric strike to ensure full operation of door latch.

.23 Glass Break Sensor

- a. Shall be installed within 6100mm of the glass that the sensor monitors

.24 Access Control Pedestal for Parking Controls

- a. Keypad CR, and remote intercom shall be installed at appropriate height for use by driver of passenger vehicles
- b. CR shall be installed at appropriate height for use by bus and/or truck driver.
- c. Ultra long-range CR shall be installed on a separate pole; pole to be located as indicated on drawings.

.25 Cameras

- a. Each camera shall have a single ethernet connection for video feed, power, and camera control through the *LAN*.
- b. Video signals/images must not be affected by any elevator systems interference.
- c. Cameras to be zoomed out to the widest viewing angle to maximize coverage or otherwise as directed by *CS*.

3.6 INSTALLATION – SECURITY SYSTEM INTEGRATIONS

.1 System Integration

- a. Integration between the *ACS* hardware, software and *IDS* shall be seamless in both online and offline modes.
- b. The *ACS* and *IDS* are integrated locally via hard-wire inputs and outputs (see [Appendix J: Typical Lenel Security System Wiring Schematics](#)) and in software via the *WAN*.
- c. The *ACS* and *VMS* applications are integrated via the *WAN*.

.2 SCADA Integration

- a. The *integrator* shall provide 3 dry contact outputs from the IDS to the *SCADA* system for all Regional Water and Wastewater facilities:
 - i. Intrusion Alarm
 - ii. *IDS* Armed/Disarmed
 - iii. Spare
 - b. Outputs shall be configured and wired fail safe.
 - c. The Security Contractor shall coordinate integration to the Region's *SCADA* system with the Region 2 weeks in advance of the integration to have appropriate Regional representative present and to assist with the integration.
- .3 Elevator Access Control Integration
 - a. The Security Contractor shall break the "control signal" and not the "common supply" for the call button.
 - b. The *installer* shall use the spare conductors in the travelling cable, where available, when integrating *ACS* to an existing elevator.
- .4 Overhead Door and Bi-Fold door Controller Integration
 - a. The Security Contractor shall supply and install a momentary dry contact output 'request to exit' signal from door controller to associated card reader board on *ACS* for doors that are controlled by *ACS*.
- .5 Parking Controls Integration
 - a. The Security Contractor shall supply and install a momentary dry contact output from the *ACS* to activate the parking controls and shall monitor status of parking controls via dry contacts inputs (position status and alarm).
 - b. All points shall be wired fail safe.

APPENDICES

Appendix	Contents
A	Prequalified Security System Vendors
B	Security System Naming Convention Standards
C	Security System Commissioning Forms
D	Cabling
E	Pre-Approved Security Devices
F	Environmental Requirements
G	Sample Graphics
H	Camera Settings
I	Security System Labelling Requirements
J	Typical Lenel Security System Wiring Schematics

4.1 Appendix A – Prequalified Security System Vendors

- .1 The Region's only Honeywell ACAMS *integrator* is Honeywell Building Automation:

Honeywell Building Automation	Callum Marshall callum.marshall@honeywell.com (647) 455-3365
-------------------------------	---

- .2 Lenel ACAMS *integrators* prequalified under Request for Supplier Qualification Number RFSQ-755-22 (as of July 28, 2023):

360 Advanced Security Corporation	Andrew Pierce Andrew.p@360asc.com (647) 212-9654
Chubb, UTC Fire and Security Canada Inc.	Stephen Yates stephen.yates@chubbfs.ca (416) 659-1754
Paladin Technologies Inc.	Greg Cowan gcowan@paladintechologies.com (437) 684-7963
Securitas Electronic Security (Canada) Inc.	Tom Nanou Tom.nanou@securitasES.com (416) 678-7353

- .3 *Installers* pre-qualified under Request for Supplier Qualifications Number RFSQ-756-22 (as of October 31, 2023):

AC Electric	Chambers, Alex estimating@acelectricinc.ca (416) 939-0244
CEC Services Inc.	Kyle Feinstein kyle.feinstein@multitechcorp.ca (905) 713-3711
Electro-Works Ltd.	Dondi Keough dondi@tcsecure.ca (416) 529-7180
Ozz Electric	Michael Manias mmanias@ozzelectric.com (416) 989-7568

4.2 Appendix B – Security System Naming Convention Standards

All components and interconnections are to be identified by a unique name which shall be used in software (database), and on drawings, documentation and labels.

These names are to be assigned in compliance with the following parameters:

- Do not use full name on graphics, rather use device type and number.
- Commence allocation of sequential numbers/addresses from “1” for each site.

System Controllers and Panels:

E005A01 **E005** = Site Number (provided by Region)
E005I01 **A** = ACS Controller
 I = IDS Panel
 01 = Panel Sequential Number

Door:

E005D001 Z001 **E005** = Site Number
 D = CR/Door
 001 = Door Sequential Number.
 Z001 = IDS Zone Number (if applicable)

Camera:

E005C001 **E005** = Site Number
 C = Camera
 001 = Camera Sequential Number.

Glass Break:

E005GB001 Z001 **E005** = Site Number
 GB = Glass Break
 001 = Glass Break Sequential Number.
 Z001 = IDS Zone Number (if applicable)

Intercom:

E005IRS001 **E005** = Site Number
E005IMS001 **IRS** = Remote Intercom Station
 IMS = Intercom Master Station
 001 = Intercom Sequential Number.

4.3 Appendix C – Security System Commissioning Forms

The commissioning procedure is described in [Section 1.6 Testing and Quality Assurance](#).

Note that the forms are available in Excel format and should be submitted in that format. There are 11 forms:

- 1) Cover Page
- 2) ACS - Access Control System
- 3) IDS - Intrusion Detection System
- 4) Video Surveillance
- 5) Doors - Pedestrian Doors, Overhead Doors & Hatches
- 6) Gate Control (to be reviewed)
- 7) Glass Break Sensors
- 8) RFA Buttons
- 9) RFA Strobes and Piezo Buzzers
- 10) Remote Release Buttons
- 11) Video Intercom



Security System Specifications June 2025 Appendix C Commissioning Forms.xlsx

4.4 Appendix D – Cabling

1. **General**

- .1 Refer to Corporate ITS Cabling & Wiring Standard for network and video cabling requirements.
- .2 Cabling shall follow the wiring guide in Table 2 below:

Table 1 - Security System wiring guide

Purpose	Cable type	Gauge	Conductors	Description	Belden number*
RS-485	Non-plenum	24	2 Pairs	Overall shield	9842
	Plenum	24	2 Pairs	Overall shield	88102
RS-232	Non-plenum	24	5	Overall shield	9610
	Plenum	24	6	Overall shield	83506
Reader drops	Non-plenum	22	8	Overall shield	5506FE
	Plenum	22	8	Overall shield	6506FE
	Non-plenum	18	8	Overall shield	5306FE
	Plenum	18	8	Overall shield	6306FE
12 VDC power	Plenum	24	6	Overall shield	83506
	Plenum	18	2	Overall shield	6300FE, 88760
Instrumentation	Non-plenum	18	2	Overall shield	8760

*Belden cables are provided as a design basis, the *installer* may also use an approved equivalent cable

- .3 All exposed cabling must carry an FT6 fire rating.

4.5 Appendix E – Pre-approved Security Devices

APPENDIX E: PRE-APPROVED SECURITY DEVICES											
Component Type	Manufacturer	Part #	Description	Honeywell	Lenel	IDS	ACS	VMS	Intercom		
Arming Button	RCI	R991RBPTD9	Pneumatic Time Delay Pushbutton	X	X	X	X				
Button REX	RCI	991E-PTD-32D	Pneumatic Time Delay Pushbutton REX	X	X		X				
Card Reader	HID	20NKS-00-01BD08	Signo 20 Reader (mullion-mount style)	X	X		X				
Card Reader	HID	40KNKS-00-01BD08	Signo 40 Keypad Reader (single gang box mount style)	X	X		X				
Card Reader	HID	40NKS-00-01BD08	Signo 40 Reader (single gang box mount style)	X	X		X				
Communication Module	Bosch	B426	Ethernet Communication Module		X	X					
Communication Module	Bosch	B444-A	Plug-in cell communication module, 4G LTE		X	X					
Controller	Bosch	B9512G	Control Panel, IP		X	X					
Controller	Honeywell	TS3	Temaline Control Panel	X			X				
Controller	Honeywell	128BPE	Vista Commercial Intrusion Panel	X		X					
Controller	Lenel	LNL-2220	Intelligent Dual Reader Controller		X		X				
Diode	N/A	1N 4007	High Voltage Rectifier Diode	X	X		X				
Door Contact	K M Thomas	TA-4106-ES	Magnetic Door Contact, Explosion Proof	X	X	X					
Door Contact	Magnasphere	HSL-1.5-101	Door Contact, Surface Mount (UL 634 LEVEL 1) SPST			X					
Door Contact	Magnasphere	HSL-1.5-111	Door Contact, Surface Mount (UL 634 LEVEL 1) DPST			X	X				
Door Contact	Magnasphere	MSS-19C	Magnetic Door Contact, Recessed Standard Door, SPST				X				
Door Contact	Nascom	N78X/STDD	Magnetic Door Contact, Recessed Standard Door, DPDT		X	X	X				
Door Contact	Nascom	N78X/STSD	Magnetic Door Contact, Recessed Standard Door, SPDT	X	X		X				
Door Contact	Tane Alarm	SD-82	Magnetic Door Contact, Recessed Steel Door, SPDT	X	X		X				
Door Contact	Tane Alarm	SD-84	Magnetic Door Contact, Recessed Steel Door, DPDT		X	X	X				
Door Interface Relay	Camden	CX-12	Door interface relay / sequencing board	X	X		X				
Electric Strike	Assa Abloy HES	1006 xx 630	Electric Strike, Recessed	X	X		X				
Electric Strike	Assa Abloy HES	HES 9500-630	Electric Strike, Surface Mounted, Fire Rated	X	X		X				
Electric Strike	Assa Abloy HES	HES 9600-630	Electric Strike, Surface Mounted	X	X		X				
Enclosure	Bosch	B56	Keypad Surface Mount Box		X	X					
Enclosure	LifeSafety Power	E4M1	Enclosure with door and backplate		X	X	X				
Glass Break Detector	Honeywell	FG-1625F	Honeywell FlexGuard glass break detector	X	X	X					
Input/Output Module	Bosch	B208	SDI2 8-Input Expansion		X	X					
Input/Output Module	Bosch	B308	SDI2 8-Output Expansion Module		X	X					
Input/Output Module	Honeywell	RTU-A01	Digital I/O Module for up to 4 Inputs/Outputs	X			X				
Input/Output Module	Lenel	LNL-1100	Input Control Module		X		X				
Input/Output Module	Lenel	LNL-1200	Output Control Module		X		X				
Intercom Station	Zenitel	ITSV-4	HD IP Video Phone with 5" Screen	X	X				X		
Keypad	Bosch	B930	ATM Style-Alpha Numeric Keypad (SD12)		X	X					
Keypad	Honeywell	6160	Vista Series Remote Keypad	X		X					
Motion REX	Honeywell	IS320	REX Motion PIR	X	X	X	X				
Overhead Door Contact	Nascom	N205AU	Door Contact, Overhead Door	X	X	X					
Overhead Door Contact	Tane Alarm	MET-44 WG	Door Contact, Overhead Door (SPDT)	X	X	X					
Parking Gate control	Autogate	FLEX-18	Automatic Arm and Loop Sensor	X	X		X				
Pedestal	Batko	FRP-8443	Double Pedestal Pole Mount (84"/43")	X	X		X		X		
Pedestal Hood	Batko	FRH-2316	Pedestal Hood Housing for Access or Intercom	X	X		X		X		
Power Control Module	LifeSafety Power	C4/C8	Power control module 4/8 output		X		X				
Power Controller	Assa Abloy HES	2005M3	SMART Pac® III, Electric Strike In-Line Power Controller	X	X		X				
Power Distribution Module	LifeSafety Power	D8	Power distribution module		X		X				
Power Supply	LifeSafety Power	FPO series	FPO series power supply		X		X				
Reader Interface Module	Honeywell	RTU-A08	Weigand Interface Unit	X			X				
Reader Interface Module	Honeywell	TK_S014	Lonworks Weigand Interface Unit	X			X				
Reader Interface Module	Lenel	LNL-1320	Dual Reader Interface Module		X		X				
Relay	Phoenix Contact	2900329	General Purpose Relay DPDT (2 Form C)	X			X				
Relay	Phoenix Contact	2966906	General Purpose Relay SPDT (1 Form C)	X			X				
RFA Wireless Button	Bosch	RFPB-SB	Mobile Panic Button RF Transmitter		X						
RFA Wireless Button	Honeywell	F5802WXT	Mobile Panic Button RF Transmitter	X		X					
RFA Wireless Reciever	Bosch	B810	Mobile Panic Button RF Receiver		X						
RFA Wireless Reciever	Honeywell	5881EN	Mobile Panic Button RF Receiver	X		X					
Surveillance Cabinet	AXIS Communications	T98A18-VE	Surveillance Cabinet	X	X			X			
Ultra Long Range Reader	Nedap	9215689	Ultra Long-Range Vehicle RFID Reader	X	X		X				
Ultra Long Range Tag	Nedap	9882650	Ultra Long-Range Vehicle ID Window Button	X	X		X				
Video Camera	AXIS Communications	P3268-LV	Fixed Indoor Dome Camera, 3.4mm lens	X	X			X			
Video Camera	AXIS Communications	P3268-LVE	Fixed Outdoor Dome Camera, 3.4mm lens	X	X			X			
Video Camera	AXIS Communications	P3738-PLE	Fixed 360/Panoramic Indoor/Outdoor Camera	X	X			X			
Video Camera	AXIS Communications	P4708-PLVE	Dual Sensor Panoramic Camera	X	X			X			
Video Camera	AXIS Communications	P9117-PV	Dome Corner Camera, 3.4mm lens	X	X			X			
Video Camera	AXIS Communications	Q6078-E	PTZ Indoor/Outdoor Camera	X	X			X			
Video Decoder	AXIS Communications	D1110	4k Video Decoder with HDMI output	X	X			X			
Video Intercom	Zenitel	TCIV-2	IP and SIP Video Intercom	X	X				X		
Video Surveillance Monitor	ORION Image	43RCE	42.5" Full HD LED LCD Monitor	X	X			X			

4.6 Appendix F – Environmental Requirements

All security devices supplied under this contract shall meet the following environmental requirements, unless otherwise identified.

Note that these specifications are intended to address only the requirements in “normal” spaces and do not extend to the special requirements which may exist in “special” locations, such as sewage or water treatment facilities.

Outdoor Operational Environments

Air Temperature:	-40°C to +40°C
Ambient Humidity	10% to 80% RH
Wind	0 to 240 km/hr (150 mph)
Rain / Snow	up to 6 mm/min
Solar Radiation	up to 1000 W/m ²
Vibration	1.5 mm displacement, 20 m/s ² acceleration, 2 – 200 Hz
Dust	3.0 mg / m ² h

Indoor Operational Environments

Air Temperature:	+10°C to +35°C
Ambient Humidity	10% to 80% RH)
Vibration	1.5 mm displacement, 20 m/s ² acceleration, 2 – 200 Hz

Storage Environments

Air Temperature:	-45 °C (-50 °F) to 45 °C (115 °F)
Ambient Humidity	10% to 90% (RH)

4.7 Appendix G – SAMPLE GRAPHICS

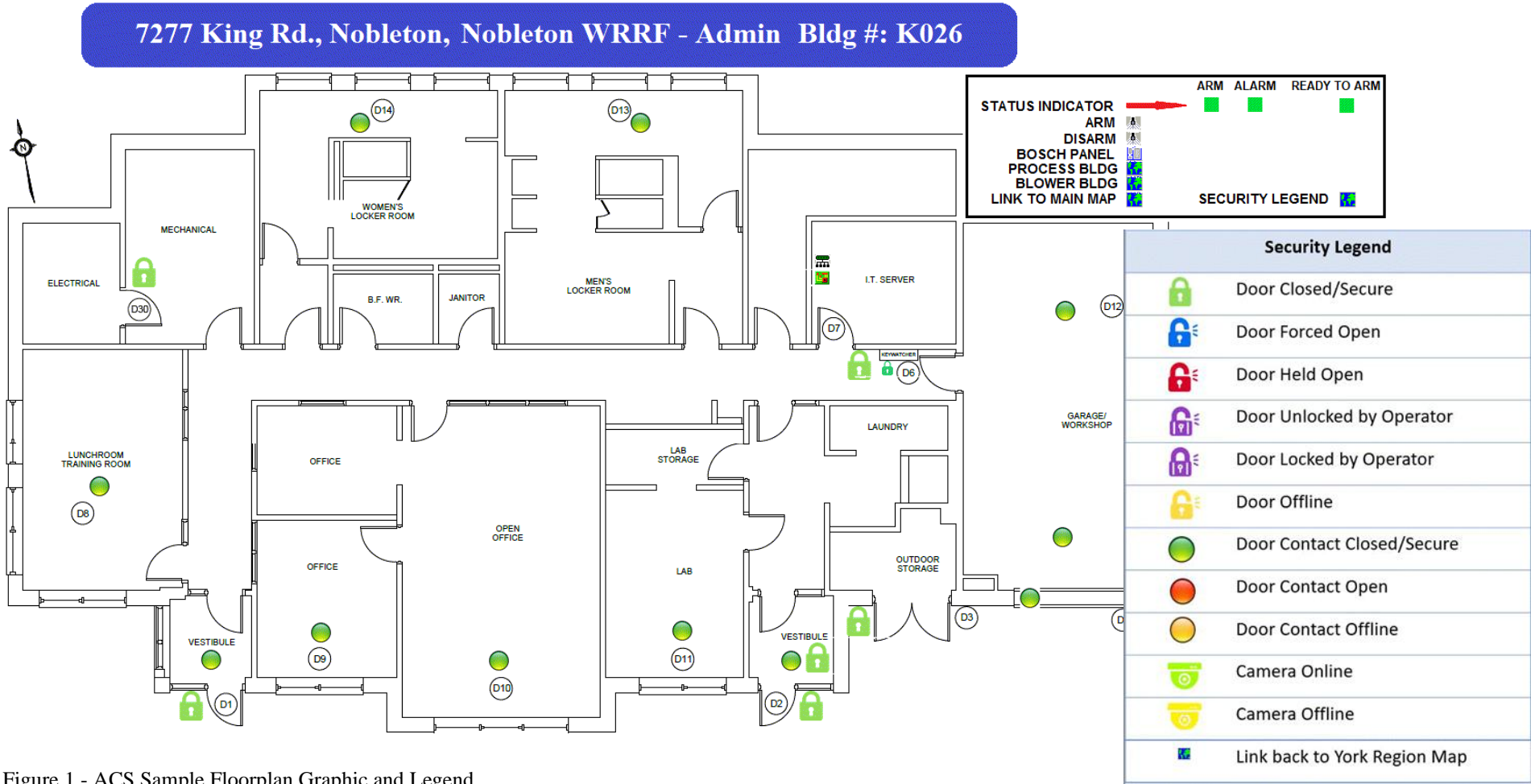


Figure 1 - ACS Sample Floorplan Graphic and Legend

4.8 Appendix H – Camera Settings

Table 2 identifies the standard settings for security cameras connected to the WAN:

Table 2 - Camera Settings

Field	Setting
Background (Stream 1) record frame rate, with motion	30 fps
Background (Stream 1) record frame rate, without motion	6 fps
Live View (Stream 2) frame rate	15 fps
Background recording duration	24 hours
Background delete after	30 days
Compression format	H.264
Compression Ratio	Medium
Resolution for PTZ	1920 x 1080
Resolution for fixed camera	1920 x 1080
PTZ preset speed	20
PTZ preset dwell time	1 second
NTP Server	172.16.1.46 & 172.16.19.47
HTTPS TLS	Disabled
Dot1x	Disabled
SNMP V2c only	Enabled
ReadCommunity: (case sensitive)	ykregion
WriteCommunity: (case sensitive)	Region Standard

4.9 Appendix I – Security System Labelling Requirements

1. General

- .1 The *installer* shall identify and label every serviceable component of the *ACAMS* including:
 - a. enclosures
 - b. cameras
 - c. network components
 - d. overhead DC
 - e. CR
 - f. cables
 - g. main alarm outputs and relays
 - h. batteries
 - i. power supplies
 - j. other components which are installed to support the *ACAMS*
- .2 All labelling shall be consistent on site, in as-built documentation and in software.
- .3 All labelling is to be permanent and legible:
 - a. Label printing shall be machine generated, at least 12-point Arial font and with black lettering on white background
 - b. Labels shall not fade or deteriorate due to exposure to the environment.
 - c. Labels to be harsh environment permanent adhesive laminated tape

2. Card Readers

- .1 Labels to be adhered to the side of the *CR* that is facing the door or gate.

3. Enclosures

- .1 Labels shall be centred from left to right.
- .2 Security cabinet shall include:
 - a. Exterior Label (on cabinet door/cover)
 - Cabinet name, as shown on the drawings
 - Cabinet purpose / nature of the equipment within.
 - b. Interior Device Labels
 - All Networked equipment is to be labelled with corresponding IP information
 - Type of Application
 - Signal source (Relay Output / Circuit / Port Number)
 - Power source (including Voltage, type of power, distribution panel and circuit number or power supply)
- .3 Junction boxes and pull boxes shall be identified with at least:
 - Nature of enclosure content, e.g., Security, Power

4. Cables

- .1 Cable labels shall be flexible cable labels of the “wraparound self-sealing” variety and of suitable size to fit the cables to which they are applied.
- .2 Identify all controller wiring at terminal blocks and connection points with the controller terminal (I/O) address numbers.
- .3 Inter-connection and terminal strips for elevator integration.

5. T-bar and ceiling

- .1 Label t-bar or finished ceiling, where equipment is installed above the ceiling.

6. Batteries

- .1 Each installed battery shall be labelled
- .2 Battery labels shall identify the date of battery install, with the date format: YYYY-MM-DD.

4.10 Appendix J – Typical Lenel Security System Wiring Schematics

1. **LENEL SECURITY PANEL WIRING AND TERMINATIONS**
 - .1 Lenel ACAMS status integration
 - a. Alarm: Connect output 1 from Bosch main panel to input 7 on Lenel site controller via contact 1 on relay 1
 - b. Armed/Disarmed: Connect output 2 from Bosch main panel to input 8 on Lenel site controller via contact 1 on relay 2
 - c. Ready to Arm: Connect output 3 from Bosch main panel to input 3 on Lenel site controller via contact 1 on relay 3
 - .2 Lenel ACAMS disarming integration
 - a. Connect output 4 on Lenel site controller to Bosch main panel input 2
 - b. Upon valid card swipe from any exterior *CR*, output 4 on Lenel site controller to fire momentarily
 - .3 Lenel ACAMS arming integration
 - a. Connect output 2 on Lenel site controller to Bosch main panel input 1 and in series with arming button and relay 3
 - b. Upon valid card swipe from any arming *CR*, output 2 on Lenel site controller to fire for 15 seconds
 - .4 NC contact on each cabinet tamper to be wired in series, to tamper input on Lenel site controller
 - .5 Connect power supply AC fault output to Lenel site controller power fault input and *IDS* via relay.
 - .6 Perimeter door hardware wiring for Lenel ACAMS
 - a. 1st pole from *DPDT* relay on *DC* for perimeter door to be connected to associated input on Lenel door controller
 - b. 2nd pole from *DPDT* relay on *DC* connected in parallel with auxiliary NO contact on associated motion *REX* and intrusion input on *IDS*
 - c. Any single pole intrusion point that also needs to be connected to ACS via relay output from *IDS*.
 - .7 Use on board ethernet for Bosch System Integration