1. GENERAL

2. PURPOSE

.1 To establish the technical, functional, jurisdictional, or regulatory and quality requirements for security and access control systems; which are required to be purchased from vendors. Approved technical specifications define the supply and installations of all security and access control systems and identify approved manufacturers and models.

.2 The security system shall consist of implementing an integrated networked Access Control and Video Assessment System (ACAMVAS) that shall control personnel access, provide real time intrusion detection alarm monitoring and provide alarm driven video surveillance for the designated buildings and operations in accordance with the requirements and specifications prescribed in these documents and the approved drawings. The security system shall include the following, where applicable:

.1 Seamless integration of a digital video management system that will allow system operators to control and maintain the security of the facilities from multiple designated client workstations.

.2 Installation and/or replacement of door and locking hardware to enable proximity card/tag reader access at designated doors. The doors designated with proximity card/tag reader access shall also allow manual unlocking using the master key system.

.3 Supply and installation of intrusion detection alarms at designated facilities.

.4 Supply and installation of interior and exterior motion detection devices to provide alarm coverage at designated facilities.

.5 Seamless integration of video surveillance systems that provides alarm driven assessment for the intrusion detection equipment at designated facilities.

.6 Supply and install proximity reader access for vehicle barriers at designated facilities.

.7 Supply and installation of all control, signal, lighting and power distribution cabling as required for the security equipment including any trenching work required for the completion of the installation.

.8 Commissioning and testing of the systems and equipment installed as required to meet manufacturers' specifications and documented installation procedures, and to the satisfaction of the Owner.

.9 Training of the Owner's personnel to: fully operate, and perform routine maintenance on the systems and equipment installed.

.10 Provide all associated documentation for the security system upgrades.

3. REFERENCE STANDARDS

.1 Underwriters' Laboratories of Canada (ULC)

.2 American National Standards Institute (ANSI) Standards

.3 Ontario Building Code

.4 CANASA (Canadian Alarm and Security Association)

.5 CFAA (Canadian Fire Alarm Association)

4. PRODUCTS

5. SECURITY COMPONENTS

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

6. ACCESS CONTROL AND ALARM MONITORING SYSTEM

.1 General System Specifications

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

.1 The system shall be a modular, networked access control and alarm monitoring system, comprised of proven commercial off the shelf components, capable of handling large proprietary corporations with multiple remote sites, alarm monitoring, video imaging, badging, paging integration, CCTV integration, interactive guard tour, mapping, visitor management, email notification, third party monitoring, BAS integration and asset management. The system shall assure long time performance, cost effective upgrade capability and allow for easy expansion or modification of inputs, outputs and remote control stations.

.2 The system control at the central computer location shall be under a single software program control, shall provide full integration of all components, and shall be alterable at any time, depending upon the requirements. Reconfiguration shall be accomplished online through system programming, without hardware changes.

.3 The Access Control Software system shall utilize Microsoft SQL Server 2000/2005/2008 for data storage and be written expressly for Microsoft SQL Server 2000/2005/2008.

.4 The system shall have the capability to be networked via a LAN/WAN connection utilizing industry standard TCP/IP communication protocol. The system shall provide encryption via the TCP/IP connection

.5 The system shall incorporate the use of bi-directional 485 communications and/or Class "A" TCP/IP redundant connections for redundancy and reliability.

.6 The system shall incorporate "High Availability" Communications so that multiple communication paths are available to all controllers. High availability shall be defined as, "an existing alternate controller shall take over communications in the event the main controller fails. The controller must be located in a separate location to the first."

.7 The system shall support both manual and automatic responses to alarms entering the system. Each alarm shall be capable of initiating a number of different actions, such as camera switching, activation of remote devices and door control.

.8 The system shall provide unlimited levels of emergency codes to allow the system to operate in different security levels depending on local threat level e.g. code black = bomb threat and building locks down.

.9 The system shall provide both supervised and non-supervised alarm point monitoring. Upon recognition of an alarm, the system shall be capable of switching CCTV cameras and automatically creating a popup window for video for the associated alarm. The system shall be capable of arming or disarming alarm points both manually and automatically, by time of day, and by day of week.

.10 Access control functions shall include validation based on time of day, day of week, holiday scheduling, site code verification, automatic or manual retrieval of card/tagholder photographs, and access validation based on positive verification of card/tag, card/tag/PIN, card/tag and video.

.11 The system programming shall be user friendly, and capable of being accomplished by personnel with no prior computer experience. The programming shall be menu driven and include online "Help" with the use of F1 hotkey to automatically call the proper help information to the screen. The software shall utilize drop boxes for all previously entered system required data.

.12 After installation, the Owner shall be able to perform basic hardware configuration changes. These hardware configuration changes shall include, but not be limited to, door open time, door contact shunt time, point and reader names, when and where a card/tagholder is valid, and the ability to add or modify card/tag databases as desired without the services of the Manufacturer or Manufacturers Dealer.

.13 Equipment repair shall be able to be accomplished on site, by module replacement, utilizing spare components. All equipment shall have unplugable connectors for easy replacement.

.14 All control components shall include the ability to download operating parameters to any control panel, thus allowing the control panel to provide full operating functions independent of any other system component.

.15 The system shall be designed in such a way that it does not require enrolment of authorized personnel at each building.

.16 The system shall provide seamless integration to multiple manufacturers of DVR's and NVR's at the same time.

.17 The system shall provide seamless integration with external building control systems (BAS) , personal safety systems, remote paging and email systems.

.18 All system events, operator actions and maintenance information shall be stored on the computer hard disk to maintain a permanent record of system activity. The system shall have the capability for manual and automatic

back-up of set-up and system events to either local removable media (optical/magnetic) or remote network resource.

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

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

.2 INTERACTIVE MAPPING AND GRAPHICS

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

.3 INFORMATION STORAGE

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

.4 INFORMATION BACKUP/RETRIEVAL

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

.5 COMMUNICATION RATES

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

.6 PRINTERS

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

.7 POINTING DEVICE

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

.8 COMMUNICATION PORTS

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

.9 WORKSTATIONS

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

.10 NETWORKING

The system shall operate with the standard Windows networking software.

.11 DATABASE

The database shall be Microsoft SQL Server2000/2005/2008.

.12 SOFTWARE CAPACITIES

.1 The System server shall have the following minimum requirements. Windows 2000, WIN XP Pro, Server2003, Server 2008, Windows 7 Business, with 2.2ghz clock speed, 2gig Ram, 40 gig hard drive, CD Rom, Pointing device and video graphics card with 512 on board ram.

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

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

- Unlimited reader expansion
- Unlimited card/tagholders in software
- Unlimited simultaneous client PCs
- Unlimited time zones
- 365 user-definable holidays
- Unlimited Access levels
- Access levels for each card/tagholder
- Unlimited alarm input points
- Unlimited output control points
- Unlimited operator passwords with definable privilege levels
- Audible alarm annunciation at the CPU
- Unlimited color graphic maps displayed on the CPU monitor
- TCP/IP or RS232 interface capability to a CCTV system, which provides automatic, alarm actuated camera switching.
- True 32/64 bit operation
- Operator activation/cancellation dates
- Employee activation/cancellation dates
- Optional Video Imaging/Badging & bar code imprinting

.13 SYSTEM ADMINISTRATORS SHALL HAVE THE FOLLOWING ABILITIES AS A MINIMUM:

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

.14 ALARM WINDOW DESCRIPTION

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

.15 BULK ACKNOWLEDGMENT OF ALARMS

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

.16 STATION ROUTING

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

.17 OPERATOR ROUTING

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

.18 MENU CONFIGURATIONS

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

.19 MEMORY

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

.20 DATABASE UPDATES

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

.21 REPORTING

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

.22 WORKSTATIONS

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

.23 SERIAL PORTS

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

.24 TIME ZONES

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

b) The time zones shall be assignable to:

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

- Printer operation
- Workstations

.25 HOLIDAYS

The system software shall support a minimum of 365 holidays. Holidays shall be considered HI or H2 designation so that there are three distinct holiday times. A holiday shall be capable of starting at any time/hour during a 24-hour day. Systems requiring holiday start time of midnight shall not be acceptable.

.26 DOOR DESCRIPTIONS

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

.27 ACCESS CONTROL MODES

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

- "CARD/TAG ONLY"
- "CARD/TAG + PIN"
- "PIN ONLY"
- "HIGH SECURITY"
- "TWO PERSON"
- "FREE ACCESS"

.28 DURESS

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

.29 DOOR ALARMS

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

.30 DOOR ALARM ANNUNCIATION

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

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

.31 ALARM DESCRIPTION

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

.32 ALARM ENABLING

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

.33 ADDITIONAL ALARMS

The system must also generate alarms for the following:

- Enclosure tampering
- Controller panel communication loss
- Channel 1 Fail /Channel 2 Fail
- Battery Failure

- AC Failure
- Reader Fuse
- Auxilary Fuse
- Lock Fuse
- Alarm tampering (supervised)

.34 ALARM SUPERVISION

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

.35 ASCII OUTPUT:

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

.36 OUTPUTS

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

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

.37 ENCRYPTION

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

.38 OPERATOR ACCESS LEVELS

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

.39 PASSWORD SECURITY

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

.40 PARTITIONING

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

.41 OPERATOR ACCESS LEVELS

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

- General Administrator
- Supervisor
- General User

Privilege levels shall be assignable to, but not limited to the following menu functions:

- View
- Edit
- Edit of any field within the menu
- Select

.42 OPERATOR ACTIVITY

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

.43 AUDIT TRAIL OF DATABASE CHANGES

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

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

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

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

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

.44 EMPLOYEE DEFINITIONS

.1 Card Entering:

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

.2 Card/tag Data:

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

.3 Employee records:

Employee records shall consist of a minimum of the following:

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

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

.4 Batch Loading:

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

.45 REPORTS

.1 Data Storage:

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

.2 System Function:

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

.3 Media:

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

.4 Search Criteria:

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

.5 Report Types:

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

- Card/tagholder data
- Door groups

- Time zones
- Doors
- Inputs
- Relays
- Links
- Controller panels
- Operators
- System hardware configuration
- System settings configuration

.6 Transaction Reports:

Transaction reports shall be available for the following:

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

.7 Report Scheduling:

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

.46 SYSTEM GUIDES

.1 On Line Help:

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

.47 SYSTEM STATUS

.1 Real Time Status:

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

- Inputs
- Outputs
- Doors

.2 Alarm Monitor:

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

.48 GRAPHICS

.1 Graphics File Format:

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

.2 Programming:

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

.3 Operation:

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

.49 VIDEO BADGING

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

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

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

.50 VIDEO IMAGING

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

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

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

.51 DVR AND NVR INTEGRATION

.1 The system shall integrate seamlessly via TCP/IP to multiple manufacturers DVR's and NVR's simultaneously. The operator shall have the option to associate any camera with a device and through a common video window, control, and operate any device with real time viewing. Video shall be accessible from any device via a right mouse click. Video history of any event shall be accessible via a right mouse click. The video window shall automatically pop-up upon activation of the associated device's alarm. Video shall be common to all manufacturers systems so that the operator only sees one view.

.52 INTERACTIVE GUARD TOUR:

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

.53 ASSET MANAGEMENT:

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

.54 SYSTEM TOOLS

.1 Copy Wizard

The system shall provide a copy wizard to quickly copy any device parameter to any other single or group of devices.

.2 Back-up Scheduler

The system shall have a backup scheduler for automatic backup of data

.3 Custom Cardholder fields

The system shall have the ability to custom design the cardholder data by adding new fields at will.

.55 BIOMETRIC/FINGERPRINT ENROLLMENT

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

HARDWARE - AXIOMV CONTROLLER PANELS

3 UNC500 TCP/IP CONTROLLER

3.1.1 The controller panel shall be a 32 bit microprocessor controlled solid-state electronic device and shall include a real time clock/calendar on board. Boards shall be made of gold plated construction (Copper or leaded will not be accepted) and incorporate flashware technology. Communication shall Two channel TCP/IP standard LAN/WAN windows environment protocol. A subset of the system database sufficient to support access and alarm functions for its designated readers and points shall be stored at the controller panel. In event of communication loss, the controller panel shall continue to function without degradation of operation and shall provide storage of a least 10,000 events. These stored events shall be uploaded to the CPU automatically upon restoration of the communications. The system shall be capable of performing all system functions indefinitely without the computer.

3.1.2 The controller must be FCC, CE, RoHS and UL listed.

3.1.3 The controller must have 8mb Ram available on board

3.1.4 The controller must have 65,000 offline event buffer

3.1.5 The controller must have 3 programmable RS485 ports

3.1.6 The controller must have 2 on board weigh and reader ports to accept any weigh and format and 5 weigh and formats simultaneously.

3.1.7 The controller must have 8 fully supervised inputs capable of individual configuration for EOL (single and dual EOL), N.O, N.C. operation.

3.1.8 The controller must have eight outputs. 4-form 'C' relay outputs rated at 10A-30VDC and 4-open collector 100ma outputs.

3.1.9 The controller must have two on board TCP/IP LAN connections capable of configuration in LAN switch mode or dual LAN operation for Class 'A' Communication configurations.

3.1.10 The Controller must have separate tamper input

3.1.11 Input voltage 12vdc or 30w P.O.E. maximum current draw 500ma

3.1.12 The controller must have internal charging circuit for 12vdc gell cell standby battery. The controller shall be capable of recharging a standby battery from either P.O.E. source or 12v local power supply.

3.1.13 The controller shall be configurable in the following methods. Edge device, Wall mount controller or Rackmount.

3.1.14 Edge device deployment shall be POE and operate continuously even if POE is lost. Edge controller shall operate 1 or 2 doors as desired.

3.1.15 Rackmount configuration shall be two UNC500 controllers or 4 doors in a standard 1U- 19inch rack configuration. LAN connections shall be front facing as standard Network configuration. All device connections shall be independent and removable from the rear of rack for quick disconnect and easy troubleshooting. All rackmount cabinets shall have optional rails for slide out configuration. All rackmount cabinets shall have top removable panel to access control panels.

3.1.16 The controller when configured in switch mode shall allow LAN looping from one standard windows device to another as any standard network switch allows without the use of external switches or special LAN cabling.

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

4 NC100 CONTROLLER:

4.1.1 The controller panel shall be a 32-bit microprocessor controlled solid-state electronic device and shall include a real time clock/calendar on board. Boards shall be made of gold plated construction (Copper or leaded will not be accepted) and incorporate flashware technology. Communication shall be bi-directional with speeds up to 2.5mb/s. A subset of the system database sufficient to support access and alarm functions for its designated readers and points shall be stored at the controller panel. In event of communication loss, the controller panel shall continue to function without degradation of operation and shall provide storage of a least 10,000 events. These stored events shall be uploaded to the CPU automatically upon restoration of the communications. The system shall be capable of performing all system functions indefinitely without the computer.

4.1.2 The controller panel shall be capable of operating over a LAN/WAN using Ethernet TCP/IP. The individual controller panels can be networked together along with the CPU to provide fast, real time updates and uploads/downloads using Ethernet TCP/IP.

4.1.3 The controller panel shall be capable of communicating via a RS232 link directly to the system CPU. No additional interface equipment shall be required. The distance between control panels shall be up to 4000 feet.

4.1.4 The controller panel shall have an LED display to indicate the following: power, battery backup, AC status, Auxiliary Status and the transmitting and receiving of programmed data.

4.1.5 The controller panel shall include, as standard, at least four (4) hours of battery backup for the controller panel. The controller shall use a battery save circuit to save batteries in the event of undue extended power fail. The controller panel shall include internal auto recharge battery backup to maintain system operation. Upon power loss mag locks, electric door strikes, etc. shall be fail secure.

4.1.6 The controller panel shall support four (4) reader controllers with 2 reader ports on each reader controller. Reader ports shall read any weigh and input and up to five formats simultaneously. Reader ports shall allow a keypad to be used in conjunction with the reader and utilize user-definable PIN codes. Systems requiring additional ports for the addition of a keypad are not acceptable. The controller panel shall be able to support multiple card/tagcard/tag/tag technologies (Proximity, Magnetic Stripe, Weigh etc.) concurrently without additional software or hardware.

4.1.7 Links are defined as any action causing any reaction on the system. Each controller shall be capable of initiating 'Links' regardless of the computer status.

4.1.8 Readers shall have the ability to initiate s swipe and or 4 swipe commands based on user card programming to initiate a different sequence of events depending on the need.

4.1.9 Each controller panel shall, without additional hardware, monitor at least eight (8) alarm inputs.

4.1.10 Each controller panel shall, without additional hardware; control four (4) user-definable form "c" relay outputs and four user definable transistor outputs for eight.

5 RBH-IOC-16 INPUT OUTPUT CONTROLLER

5.1.1 Additional inputs and outputs shall be available by adding IO boards. Each expansion board shall have a minimum of sixteen (16) supervised inputs or outputs. The inputs shall incorporate full supervision of 7 circuit types and the outputs shall be form "C". Up to sixteen (16) expansion boards shall be available for each controller panel.

5.1.2 The IO board shall be independently powered and have its own back up power supply and charging circuit for a minimum 4 hour standby operation.

6 RBH- ENCL2 WALL CABINETS

6.1.1 The controller panel enclosure shall have a hinged cover with key lock. A control panel input point shall monitor an enclosure tamper switch.

6.1.2 The cabinet shall be 22" X 18" X 4" with ½ and ¾ inch knockouts. The back of the cabinet shall have key mounts for easy mounting.

6.1.3 The cabinet shall hold any two of the following controllers UNC500, NC100, RC2, IOC16

7 NC100 CONTROLLER PANEL FIRMWARE FEATURES

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

7.1.2 The controller panel shall be capable of storing up to eight (25) custom card/tagcard/tag/tag formats and reading 5 formats simultaneously. The controller panel shall be able to read the format of most Magnetic Stripe, Bar Code, Proximity or Weigh and Effect encoded card/tagcard/tag/tags and shall allow an operator to specify parity, start sentinels, stop sentinels, field separators, facility code bits, issue level bits, and card/tagcard/tag/tag number bits.

7.1.3 The controller panel shall be capable of reading card/tag numbers up to eighteen (18) digits.

7.1.4 The controller panel shall have the capacity to store up to 128 time zones with each time zone consisting of up to 16 intervals of time. Each interval of time shall consist of a range of days (seven days of the week, in addition to a Holiday Schedule) as well as a range of time. The controller panel shall automatically manage time zones based upon its internal clock.

7.1.5 The controller panel shall allow for the definition of up to 365 Holidays. Holidays shall be defined according to day of year and time of day. All holidays shall be automatically incorporated into Time Zone definitions.

7.1.6 Each card/tag reader/keypad shall have the ability to independently operate in up to six different modes: Card/tag reader only, PIN only, Common Code only, Card/tag Reader plus PIN, High Security and Free Access. These modes of operation shall be programmed from the system host computer and shall automatically change by time zone assignment.

7.1.7 The system shall support interlock groups for Man –trap operation.

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

8 CARD/TAG READERS & CARD/TAGS

8.1.1 The system shall employ a proximity access control/identification technology that utilizes radio frequency (RF) circuits in microchip form. The microchips are encoded and transmit the encoded information when activated.

8.1.2 The readers shall be any weigh and output or equivalent proximity/iclass/mifare type. It shall read the identification number of the card/tag or tag when presented to the surface of the reader without physical contact.

8.1.3 Single piece window/door frame reader, which shall mount directly on a standard 1.75" (4.5cm) metal mullion/door frame. The reader can be mounted indoors or outdoors on virtually any surface, including metal. The reader shall operate between 5 volts and 14 volts DC to allow for ease and flexibility in installation. Read range with a standard proximity card/tag shall be up to 4" (up to 10cm) when installed according to manufacturer’s specifications. Maximum dimensions of the reader shall be 5.5" (14.0cm) High x 1.6" (4.1cm) Wide x 0.75" (1.9cm) Thick.

8.1.4 A single piece wall switch reader, which shall mount directly on a standard metal or plastic single-gang electrical box, or on a flat wall or metal surface, and shall operate indoors or outdoors. The reader shall operate between 5 volts and 14 volts DC to allow for ease and flexibility in installation. Read range with a standard proximity card/tag shall be up to 4" (10cm) when installed according to the manufacturer's specifications. Maximum dimensions of the reader shall be 4.6" (11.7cm) High x 2.9" (7.6cm) wide x 0.5" (1.3cm) Thick.

8.1.5 A single piece reader, which shall mount to any surface, including metal, or can be concealed behind most building materials, except metal. Read range with a standard proximity card/tag shall be up to 7" (17cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader shall be 4.6" (11.7cm) High x 5.5" (14cm) Wide x 1.4" (3.6cm) Thick.

8.1.6 A medium range reader, which shall mount to most surfaces, except directly on metal, or can be concealed behind most building materials, except metal. Read range with a standard proximity card/tag shall be up to 21" (42cm) when installed according to manufacturer's specifications. Maximum dimensions of the reader head shall be 8.8" (22.4cm) High x 8.8" (22.4cm) Wide x 1.14" (2.9cm) Thick.

8.1.7 The card/tag or tag shall be read when presented in any orientation or at any angle to the surface of the reader within the proper read range

8.1.8 The reader shall power the card/tag or tag, process the encoded data, and output the data to the access system in less than 110 milliseconds.

8.1.9 There shall be no removable plate or cover, which allows access to the reader electronics.

8.1.10 A red/green LED on the front surface of the reader shall indicate to the user that the card/tag or tag was read (internal/reader controlled) and an access decision was made (system controlled). The LED may be configured in either single line mode or dual line mode (allowing an "off" state) as required by the host system, and the reader may be switched between modes by presenting a programming card/tag to the face of the reader.

8.1.11 The reader shall have an audio "beep" tone feature to indicate to the user that the card/tag or tag was read (internal/reader controlled) and an access decision was made (system controlled). The audio tone must be independently controllable and not tied to the status or color of the LED. The internal control of the LED and beeper may be enabled/disabled via programming card/tags so as not to require the setting of switches internal to the reader.

8.1.12 The reader shall have a built-in diagnostics, which indicate to the installer that upon power up the reader has performed an internal test and is functioning properly.

8.1.13 The reader shall have a built-in diagnostic feature, which allows a single technician to test the continuity of the data lines independent of the door controller. The reader may be placed into the line diagnostic mode via a programming card/tag, and the technician can then measure the pulses at the end of the line without the need of a second technician at the reader presenting card/tags.

8.1.14 Electrical connections between the reader and the controller shall be via color coded, multiconductor; #22 AWG shielded cable. No coaxial cable or special connectors shall be required. The output shall be in the form of Weigh and data stream.

8.1.15 Wiring from the reader assembly to the system interface or CPU shall be run inside metal conduit or EMT, as may be required by electrical codes. All junction boxes are to be concealed and bot normally accessible to the public. Utilization of PVC conduit is not acceptable.

8.1.16 Accidental or intentional transmission of radio frequency signals into the reader shall not compromise the system.

8.1.17 The reader shall function in the access control system's normal or anti-passback mode without changes to the reader.

8.1.18 The reader operating temperature range shall be -40° to +50° C

8.1.19 Damage or vandalism to the reader shall not damage any other part of the system.

8.1.20 Tampering with the reader shall have no effect on the door security.

8.1.21 The system readers shall have the capability to accept codes from any of the following proximity devices:

8.1.22 A standard molded plastic credit card/tag sized card/tag having maximum dimensions of 3.41" (8.7cm) x 2.14" (5.4cm) x 0.09" (0.23cm), and a weight of not more than 0.48 oz. (13.5g). A punched slot shall be provided for a strap or clip. The card/tag shall be capable of having multi-colour custom graphics and permanently marked numbers printed directly onto both sides.

8.1.23 A tag having maximum dimensions of 2.2" (5.6cm) x 1.3" (3.3cm) x 0.25" (0.6cm), and weight of 0.36 oz. (9.9g). A brass eyelet shall be provided for attachment to a key ring.

8.1.24 A credit card/tag sized card/tag made of PVC, having maximum thickness of .036", and the capability of accepting direct print video imaged graphics and photographs and able to carry a high coercivity magnetic stripe.

8.1.25 A credit card/tag sized card/tag having maximum thickness of .048", and capable of accepting a photograph and graphics via a customer laminated flap.

8.1.26 The card/tag shall be a polycarbonate-based card/tag that cannot be run through direct card/tag printers. The card/tag shall be a PVC dual technology card/tag that employs proximity sensor technology. It shall comply with ISO standards for thickness (30 mil).

8.1.27 The card/tag or tag shall be made of robust ABS plastic to provide maximum protection for the circuitry inside and provide minimal flexing which could cause damage to the card/tag.

8.1.28 The presence of small metal objects, such as keys or coins near the card/tag or tag shall not alter the code read by the reader, nor prevent the code from being read by the reader.

8.1.29 The card/tag shall be of a proprietary format to be controlled by the Owner.

8.1.30 Card/tags or tags shall be sequentially numbered. The user may specify codes or numbers.

8.1.31 The card/tag must have the ability to have the encoded number permanently marked on the outside surface.

8.1.32 The card/tag or tag shall be a passive device with no internal battery, but shall contain a semiconductor element, which is energized when brought within the operating range of the reader causing transmission of the code from the card/tag or tag to the reader. Card/tags requiring an internal battery or energy cell shall not be acceptable.

8.1.33 Card/tags and tags may be used interchangeably and shall be compatible with all readers in the system, regardless of the reader's physical size or style, and without any code matching or memory devices in the reader.

8.1.34 The card/tag and tag operating temperature range shall be -40° to +50° C

9 FINGERPRINT/BIOMETRIC READERS AND SOFTWARE INTEGRATION

9.1.1 The fingerprint reader shall be RBH-BIO

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

9.1.3 The capture template will allow the capture of a primary and secondary finger as a backup.

9.1.4 The authentication will be automatically downloaded to the reader upon successful capture of the fingerprint without intervention by the operator. The download shall be by TCP/IP communications to the fingerprint readers.

9.1.5 The fingerprint must be saved as an algorithm to protect individual privacy.

9.1.6 The fingerprint algorithm shall be saved within the normal AxiomV database for automatic backup and restore capabilities. External backup systems for fingerprint are not acceptable.

9.1.7 The fingerprint reader shall be configurable to operate in any of the following modes. Finger only, card plus finger, Finger plus PIN code.

9.1.8 The reader shall have a weogand output to connect to the door control panel

10 ACS VMS INTEGRATION

10.1 Integration must be through TCP/IP (relay and or RS232 connections are not acceptable).

10.2 All devices within the ACS system must have a tab to associate a video camera from the VMS system to the device. This association must allow the camera to be called into the ACS GUI upon the following conditions. A) Any Incoming event from specified device B) Any incoming alarm from the specified device. The camera if PTZ must also be called to its predesignation preposition.

10.3 The ACS must be able to connect to the VMS system and display the VMS's default video window as a native VMS viewing client.

10.4 The ACS must have the ability to pop-up any video event designated for pop-up without operator intervention.

10.5 The ACS must have the ability to manually call video by clicking on the event anywhere it appears in the ACS.

10.6 The ACS must have the ability to dynamically place the cameras from the VMS system on its maps and call video from the maps directly.

10.7 The ACS must have the ability to report all events tagged with video and play back directly from the report within the ACS GUI.

11 ALARM KEYPADS

11.1.1 The system shall incorporate alarm keypads that link directly to the system for advanced alarm operation. Integration to third party alarm systems are not acceptable. Operators can arm, disarm, send messages and monitor any alarm on the keypad. In addition the keypads shall have entry exit zones and the ability to initiate commands on the system by entering a code or command. The keypads will have the ability to arm or disarm any group of inputs on the system creating a seamless alarm intrusion panel.

11.1.2 Alarm Monitoring Integration:

11.1.3 The system shall allow for annunciation of intrusion detection alarms. Intrusion detection alarms shall report just like any other access control alarm and shall have the same annunciation and display properties as access control alarms.

11.1.4 Alarms from the alarm keypad shall be displayed in the alarm-monitoring window and any signal can be sent out via TCP/IP or RS232 message port.

11.1.5 7BThe system shall support an Alarm Details description that shall show the 'Alarm Description', 'Time/date', 'Controller', 'Device', and 'Area' associated with the alarm. The information shall also display the user.

11.1.6 The system shall support tracing of intrusion detection devices and areas.

11.1.7 The system shall be able to report status information for the intrusion detection devices.

11.1.8 On alarm, the system shall automatically switch to the map that displays the alarm, the icon that represents that alarm point will flash and an audible alert will be generated on the computer sound system. The operator shall have to acknowledge the alarm before processing the alarm.

11.1.9 In operator alarm mode processing, the system shall allow the operator to:

11.1.10 Clear alarm, tamper, and diagnostic alarms

11.1.11 Observe CCTV camera views, individually or in groups, that are associated with an alarm (requires video switcher option)

11.1.12 In operator normal mode processing, the system shall allow an operator to:

11.1.13 View a list of activity information, and select and tag any event

11.1.14 View site maps

11.1.15 Perform a test of testable devices/sensors

11.1.16 Change the state of sensors to access or secure

11.1.17 Review the last 1000 events/actions performed on the system

11.1.18 In maintenance processing, the system shall allow the maintenance technician to:

11.1.19 Assign passwords and function access to individual users

11.1.20 Examine the input/output point states

11.1.21 Adjust the sensitivity of the sensors

11.1.22 Access the operating system to diagnose system problems

11.1.23 Set the calendar clock's date and time (in Windows)

11.1.24 Change the format of the displayed date (in Windows)

11.1.25 Set the communication parameters for system devices

11.1.26 Shut down the system

12 INSTALLATION

12.1.1 The contractor shall install all system components in accordance with the manufacturer's instructions, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. Power, control, signal and communications, and data transmission lines plus all required grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation. Provide mounting hardware as required.

12.1.2 All products, software, programming tools, etc. shall be registered to The Owner and will be surrendered upon successful completion of the project.

12.1.3 All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code. Cable shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring.

12.1.4 All inputs shall be protected against surges induced on device wiring. Outputs shall be protected against surges induced on control and device wiring installed outdoors. All communications equipment shall be protected against surges induced on any communications circuit. All cables and conductors, except fibre optics, which serve as communications circuits from security console to field equipment, and between field equipment, shall have surge protection circuits installed at each end.

12.1.5 No wiring or cabling shall be exposed; all wiring and cabling must be fully enclosed in threaded metallic conduit, which shall be installed underground, in walls or metal structures unless physically impossible. Any conduit that is exposed shall be fully enclosed within an expanded metal protective cage that is vandal resistant and is equipped with a tamper alarm. All equipment mounting is to be such that the equipment cannot be removed or tampered.

END OF SECTION