

Infinias, Inc

Electronic Access Control System V4.0

Architectural & Engineering Specifications

Version No. 131004

Contact Us

9340 Priority Way West Drive, Indianapolis, IN 46240

Tel: 317.348.1086 / Toll Free: 866.496.5783 / Fax: 888.52737506

www.infinias.com



PART 1. NOT USED

PART 2. PRODUCTS

2.01 GENERAL

A. Contractor Responsibility

All products not provided by [Client] shall be new and unused, and be provided from the manufacturer's current and standard production. Where two or more equipment items of the same kind are provided, all shall be identical and provided by the same manufacturer. Drawings and specifications shall indicate major system components, and may not show every component, connector, module, or accessory required to support the operation specified. Contractor will provide all components needed for complete and satisfactory operation.

2.02 PRODUCT AVAILABILITY

A. Prior to proposal

Contractor, prior to submitting a proposal, shall determine product availability and delivery time, and include such considerations into his proposed contract time.

B. Product acquisition

Certain products specified may only be available through factory-authorized dealers and distributors. Contractor shall verify his ability to procure the products specified prior to submitting a proposal.

C. Wire and Cable

1. Installation

All wire and cable required to install systems shall be provided as indicated. Wire and cable shall be sized to provide minimum voltage drop and minimum resistance to the devices being supplied.

2. All cables will be specifically designed for their intended use (direct burial, aerial, etc.).

3. All wire and cable will comply with the equipment manufacturer's recommendations for wire and cable.

4. Color codes will be consistent in cables used for the same purpose.

5. All wire and cable will comply with all applicable codes and ordinances.

6. All Power over Ethernet (PoE) cable will be either Cat 5 or Cat 6.

D. Conduit and Raceway Systems

1. General: [Client] shall approve the placing of surface mounted conduit on the exterior of any building prior to its installation.

2. All interior and exterior conduit and raceway systems used shall be compliant with applicable codes and ordinances.

3. Interior Conduit

a. Electrical metallic tubing (EMT)

b. Flexible Metal Conduit

c. Provide fittings and connectors as required for installation of EMT or flexible conduit.

4. Surface Raceways

a. Sheet metal channel with fitted cover, suitable for use as surface metal raceway, Wiremold or approved equal.

b. Provide fittings, elbows, and connectors designed for use with raceway system.

5. Exterior Conduit
 - a. Rigid steel conduit
 - b. Rigid aluminum conduit
 - c. Rigid nonmetallic conduit (only if buried 18 inches below ground surface).
 - d. Intermediate metal conduit
 - e. Provide rain-tight fittings and connectors as required for installation of exterior conduit.
6. Exterior Flexible Conduit
 - a. Liquid-tight flexible conduit: Flexible metal conduit with PVC jacket.
 - b. Provide rain-tight fittings and connectors as required for installation of Liquid tight Flexible Conduit.
- E. Junction and Pull Boxes
 1. Interior Boxes; Sheet Metal Outlet Boxes: Sizes are determined in accordance with code requirements for conductor fill. No box will be smaller than a single gang 1-1/2 inch deep. Box covers will be provided as required.
 2. Exterior Boxes: All exterior boxes shall be NEMA 4 or NEMA 3R, watertight and dust-tight.
 3. Controller Boxes: All controller boxes provided are 2-gang boxes.
 4. All interior and exterior box covers will be fastened using security screws.
- F. Lightning Protection
 1. The Contractor shall provide suitable lightning protection for all EAC equipment.
 2. All lightning protection equipment will be UL Listed.
- G. Surge Protection
 1. The Contractor shall provide suitable surge protection for all EAC equipment.

2.03 ELECTRONIC ACCESS CONTROL AND ALARM MONITORING SYSTEM EQUIPMENT

- A. Functional Requirements
 1. General
 - a. The system infrastructure shall be of a modular type, capable of allowing future expansion.
 - b. The security system encompasses the following subsystems:
 - 1) The access control and alarm subsystems shall execute functions related to access control, site and door surveillance, motion detection, intrusion, glass breakage, and external alarm sensing, such as fire alarms.
 - 2) The imaging subsystem, linked to the access control/alarm subsystems, shall be capable of printing an image and data on cards using the same system database.
 - 3) The card access control subsystem shall be composed of three hierarchy levels:
 - a) Access controllers that control supervision and command functions.
 - b) A control station that monitors alarms and responds in real time to all information in a user-friendly manner.
 - c) A group of peripheral devices, installed in areas requiring protection, each dedicated to their specific function.
 - c. All databases have the ability to do the following:
 - 1) Add, modify, view, or remove information.
 - 2) Provide storage of all system transactions in a retrievable file.

- 3) Log all events by time and date.
- 4) Log on to the software by means of valid user name and password.
- 5) Make system configuration changes such as, but not limited to, door open time, door open too long, point and reader names, when and where a card holder is valid, and the ability to add or modify card databases at any time.
- 6) Provide the ability to configure event display, alarms, e-mail and SMS notification based on one or more of schedule, group, zone, event type and resulting action at the door.
- 7) Allow for configuration of rules based on incoming events that lock a zone, lockdown a zone, unlock a zone or revert to the current unlock schedule.
- 8) Provide the ability for manual operator control of system outputs. The manual functions shall include the ability to energize, de-energize, and return to original state.
- 9) Provide the ability for manual operator control of system inputs. The manual functions shall include the ability to bypass and un-bypass.
- 10) Provide the ability for manual operator control of system access services. The manual functions shall include the ability to lock, unlock, and set door to default schedule.
- 11) Provide the ability for manual operator control of system alarm services. The manual functions shall include the ability to arm, disarm, and return the alarm zone to default schedule.
- 12) Provide the ability for manual operator control of system arming services. The manual functions shall include the ability to arm, disarm, and set alarm zone to a schedule.
- 13) Provide the ability for manual operator control of system equipment services. The manual functions shall include the ability to activate, deactivate, and set equipment service to default schedule.
- 14) Provide the ability to easily check status of each door including whether the controller is available or initializing, the controller configuration is current, if the door is locked or unlocked and open or closed. Variations on these statuses shall indicate if the state is normal or extraordinary, such as a lock that is overridden with lockdown preventing access through the door.
- 15) Provide the ability to remotely update controllers and other units with revisions of the firmware program. Devices shall be fully reprogrammable so their internal software features can be updated when new revisions of the device's system firmware are released.

2. Card Technology Supported

The system provides support a several card (credential) formats and allows customization of the formats in the system including, but not limited to, the following:

- a. Select Wiegand formats from 15–64 bits
- b. HID Prox compatible (125 KHz) key code formats
- c. 26 bit key code with custom site code and card numbering for HID ISOProx II cards, ProxKey II cards and ProxKey III
- d. 26 bit key code compatible with HID DuoProx II, HID ProxKey II, ProxKey III Keyfob credentials

3. Card Types Supported

The system provides support for several card and keyfob credentials compatible with the supported card readers including, but not limited to, the following:

- a. Xceed (HID Prox compatible) part numbers 7410, 7510, 7510C, 7510H, 7510M1, 7610, 7710-D35, 9420, 9520, 9520M1 series cards, ISO-X Lite Secure Access Card (App only/14443)
 - b. Xceed MIFARE part numbers: 9451, 9551, 9558, 9651, 9751, 9758, 9951, 9958 memory cards.
 - c. HID part numbers 1326LGSMV, 1326LGSMV, 1351LBSMN, 1391LSSMN, 1346LSSMN (FOB), 1346LSSMN (custom numbering, keyfob), 1386LGGMN, 1324, 1386LGGM, 1336LGGMN.
 - d. HID iClass part numbers: 2080PGGMN, 2050PKNMN, 2060PKNMN, 2000PGGMN for 2 application areas, and 2002CGGMN, 2022PGGMN for up to 16 application areas.
4. Card Readers Supported
- The system provides support for several proximity and swipe card readers and readers with keypads including, but not limited to, the following:
- a. Ingersol Rand AptiQ part numbers: PR10, SM10, MT11, MT15, MTK15.
 - b. HID part numbers: 5355AGK00, 5355AGK14, 5355AGN00, 5365EBP00, 5365E1P00, 5365EGP00, 5375AGN00, 5395CB100, 5395CK100, 5395CG100, 5455BBN00, 5455BKN00, 5455BGN00, 6005B1B00, 6005BKB00, 6005BGB00.
 - c. HID Standard iClass reader part numbers: 6100CGN0002, 6100CKN0002, 6140CGN0002, 6140CKN0002, 6120CGN0002, 6120CKN0002 card readers, and 6130CGN000200, 6130CKN000200, 6130CGN000214, 6130CKN000214 readers for card and PIN use.
 - d. HID MultiClass reader part numbers: 6145CGN0002, 6145CKN0002, 6125CGN0002, 6125CKN0002, 6136CGN000200 card readers, and 6136CKN000200, 6136CGN000214, 6136CKN000214 readers for card and PIN use.
 - e. HID MultiClass Government Compliant reader part numbers: 6145CGN000A-G3.0, 6145CKN000A-G3.0, 6125CGN000A-G3.0, 6125CKN000A-G3.0 card readers, and 6136CGN000A00-G3.0, 6136CGN000A00-G3.0, 6136CGN000A14-G3.0, 6136CKN000A14-G3.0 readers for card and PIN use.
5. Other Door Devices Supported
- The Infinias system supports other devices including, but is not limited to, the following:
- a. ROFU door hardware: 2400-05 Kit, Mag Lock (standard mount), Mag Lock (mortise mount), Mag Lock (front mount), 8011-004-12-28 Delayed Egress Lock System, 2" Square "Push to Exit" LED.
 - b. BOSCH DS150i Motion Detector, DS151i Motion Detector, DS150i PIR, DS151i PIR.
 - c. GRI 29-A-W Surface Mount Switch Set, 180-12-W Steel Door Switch Set.
 - d. Stanley® EL series wireless locksets with access control.
6. Front-End Software; System Configuration
- a. The system shall have the ability to:
 - 1) Support groups and membership of a cardholder in multiple groups
 - 2) Build compound schedules for cardholders who have been granted access to specific doors or zones through their membership in multiple groups. This shall be automatic and transparent to the user.
7. Time & Schedules
- a. Schedule definitions shall include starting time, ending time, and days of the week. A schedule shall cover 24 hours by 7 days. Schedules shall allow a minimum of 3 distinct segments in one schedule. Schedules can be overridden by holiday sets and holiday schedules.

- b. Maximum number of schedules that can be created and assigned in the system shall be 4 billion.
 - c. Holiday Sets are groups of holidays. The system shall support up to 4 billion holidays and 4 billion holiday sets. Each Schedule shall support up to 7 holiday sets assigned to it for the purpose of overriding the schedule on those dates.
 - d. Each Holiday Set when assigned to a schedule can have its own 24-hour schedule.
 - e. The maximum number of holidays that can be stored on a door controller shall be 254.
8. Hardware Configuration
- a. Provide the ability to add and configure hardware modules (door controllers). A minimum of 500 door controllers shall be able to be configured.
 - b. Support auto-discovery on the server's default subnet or be configured to search on a different subnet. A list of controllers discovered on the subnet shall be listed when creating a door and shall be automatically removed from the discovered list once assigned with a door.
 - c. Encapsulate all key configuration elements of a controller/door in a set of user selectable templates with associated wiring diagrams available in the software.
 - d. Allow for the addition of new templates to the system as required.
9. Zones
- a. A zone is a physical area with a set of one or more doors that provide access into and out of that area
 - b. A door shall join two zones together
10. Groups
- a. A group is a collection of people.
 - b. A person can be a member of one group or many groups.
 - c. The system shall support up to 4 billion groups and people.
11. Privileges
- a. A privilege grants a group access to a zone on a schedule.
 - b. A group may have only one privilege per zone.
 - c. A group may have any number of privileges.
 - d. Privileges may only be assigned at a group to zone level.
12. Reports
- a. The system shall not use a proprietary reporting facility. Tools adequate to create, modify, generate and export reports shall be included in the system.
 - b. There shall be no charge for any tools required to design or modify reports.
 - c. The reporting system shall allow for reports to be run from within the system and separately.
 - d. The reporting system shall be server and browser based for viewing, printing and exporting reports.
 - e. Badges shall be designed and managed in a manner similar to reporting.
 - f. Badges shall be printable directly from the edit dialog for a person, and from the reports menu. The Reports menu shall allow badges to be printed individually or severally (batch).
 - g. Both single and dual sided badges in portrait or landscape formats shall be supported.
 - h. Barcoding in a report or on a badge of any available field shall be supported in a

minimum of 8 different formats.

13. Miscellaneous Services

- a. Database management shall be performed using the database vendor's standard toolset. The toolset shall be automatically installed on the server when the access control software is installed.
- b. An Operator's service shall allow the user to define operator privileges that shall define the operator actions that can be performed while being logged on to the application. A minimum of three role types shall be available.
 - 1) Administrator – shall be able to perform all functions within the software
 - 2) Human Resources – shall be able to see events, run reports, view door status, and perform door specific actions such as momentary lock and unlock. The HR operator shall be able to create, edit and delete people and groups, and print badges.
 - 3) User – shall be able to view events, run reports, see people and groups, monitor door status, and perform door specific actions. The User operator shall not be able to modify any data in the system.

14. Events and History

- a. All events shall be recorded in the database. The database shall have the capacity to store a minimum of 20 million events. The system shall include the ability to upgrade its database to a storage capacity of 4 billion events.
- b. A History Report search shall show the event that occurred, when the event occurred, where the event occurred, and who caused the event to occur. Video attached to events shall also be available for playback from the History screen.
- c. The administrator shall define what event will be shown on the events page. This shall include the ability to build rules based on various criteria to filter the event
- d. Events presented as Alarms on the events page shall be fully configurable by the administrator. The administrator shall have the ability to include schedules, zones, groups and event types as criteria in determining if an event is an alarm.
- e. The system shall have the ability to accept events from 3rd party systems. The administrator shall be able to define rules and actions based on those events.

B. Technical Requirements

1. Environment

- a. The system shall be designed to operate, per the requirements in this technical specification, within the following ambient conditions:
- b. Computer Components
 - 1) Temperature: 50 °F to 86 °F (10 °C to 30 °C)
 - 2) Humidity: 20% to 80%, noncondensing
- c. Components installed interior or exterior
 - 1) Temperature: -4 °F to 200 °F (-20 °C to 70 °C)
 - 2) Humidity: 0 to 95% (non-condensing)
- d. The security contractor shall take all necessary precautions to ensure the proper functioning of the system components within the above-defined ranges, or within the manufacturer's defined ranges, whichever applies.

2. System Capacities

- a. The functional capabilities shall be considered standard, without the need for add-on software or hardware.

- b. The system shall require a server with the ability to support a minimum of 20 concurrent (logged on) control locations utilizing LAN/WAN network connection.
 - d. The system minimum capacity shall be 500 readers and 10,000 cardholders,
3. System Components
- a. The complete system integrates three distinct groups of components:
 - 1) Primary Components such as the power/communication unit, door controllers, and readers.
 - 2) Secondary Components such as magnetic contacts, motion detectors, and locking devices.
 - 3) Control Stations such as the server, secondary station, and display monitors.
 - b. Primary Components
 - 1) Ethernet Access Controllers
 - a) The Ethernet access controller shall be one of recent technology, based on a microprocessor, and shall be compatible with a reader for proximity type cards. It shall have previously demonstrated its capacities in a similar access control application. It shall be capable of storing a maximum of 16,000 events in a stand-alone operation, and be capable of transmitting this information to a management system when the network is reconnected.
 - b) The Ethernet access controller shall incorporate a web browser interface server for administration of the controller through a standard Microsoft® Internet Explorer® browser. The Web page shall closely emulate the optional rich-client host software used to administer the system.
 - c) Memory for the Ethernet access controller shall be flash-based and nonvolatile. If power to a controller is lost, upon restoration of power, the unit shall retain all information contained at the time of the power loss including cardholder database, system configuration, and event transaction history.
 - d) The Ethernet access controller shall be modular and include terminations for wiring to other electronic modules.
 - e) The Ethernet controller shall communication using 10BASE-T standard.
 - f) Ethernet access controllers shall provide encryption (AES 128 Bit) at both the system level and domain level.
 - g) The following information shall be set and accessed from each controller by way of Ethernet communication:
 - (1) IP address
 - (2) Protocol used for assigning address: DHCP or Static
 - (3) Serial number
 - (4) Ability to either enable or disable Web mode (direct browser-based communication with the controller)
 - (5) Ability to provide verification/validation of a security key
 - h) The Ethernet access controller shall incorporate support for peer-to-peer communications between Ethernet access controllers. Up to 32 Ethernet access controllers shall be configured in a single domain and shall communicate peer-to-peer with each other.
 - i) The Ethernet access controller shall be equipped with an input/output port allowing communication with a network switch. If one of the Ethernet access controllers should lose power, it shall not affect the operation of the other access controllers.

- j) The Ethernet access controllers shall have the ability to acquire alarms, validate the cards, and command doors when required.
- k) The Ethernet controller shall be placed in a 2-gang box housing, recessed or surface mounted, as close as possible to the zone. The controller housing shall be secured with an anti-theft screw.
- l) The Ethernet controller shall have an integrated warning buzzer to locally signal alarms.
- m) The mounting position of the Ethernet controller within its housing shall have two levels:
 - (1) Extended: The Extended level shall allow the connection of the equipment wiring.
 - (2) Recessed: The Recessed level shall allow for the installation of the protective cover.
- n) The wiring distance between the network switch and each Ethernet controller shall be a maximum distance of 100 meters (328 feet). The VDC voltage from a Power over Ethernet (PoE) switch shall be convertible to the VDC power necessary (48 VDC [350 mA]) to maintain appropriate power to the equipment connected to the controller.
- o) An optional power source such as an external power supply of 24 Vdc (1 A) shall be available to each Ethernet controller.
- p) Address confirmation of each controller shall occur automatically without the use of DIP switches.
- q) The controller shall be able to integrate two card readers allowing for timed "hard" and "soft" anti-passback. Using peer-to-peer communications, the controller shall not require server communications for the anti-passback function to fully operate.
- r) An infrared tamper switch shall be integrated in each controller to prevent unauthorized manipulation of the equipment.
- s) LED displays shall indicate the status of the input and output points directly on the controllers to facilitate local visual diagnostics.
- t) Each Ethernet controller shall have four input points, four output points including an integrated warning buzzer, two external 12 Vdc power outputs, and two ports for intelligent proximity card reader with or without keypad.
- u) Ethernet controllers shall be capable to fulfill the following power requirements to the following connected devices:
 - (1) 12 Vdc (250 mA) to each reader
 - (2) 12 Vdc (450 mA) for a lock using an open collector relay
- v) The controller shall electronically protect output points against overloads and display them on the Event screen.
- w) The security contractor shall define the quantity of Ethernet controllers required for the building to be controlled and shall ensure that the quantity conforms to the actual needs.
- x) Ethernet controllers shall be no larger than 2.84" D x 1.70" W x 4.30" H. Operating temperatures shall be 0 °C to 54 °C (32 °F to 130 °F).
- y) The four input points shall be either normally closed (N.C.) or normally open (N.O.) programmable and shall accept optional end-of-line supervision.
- z) Two of the four output points shall share a maximum power source of 450 mA at 12 Vdc with electronic overload protection, and it shall be capable

of transferring the necessary voltage from one point to another in the event of a transition. The third output point shall be a single pull double throw (SPDT) relay type or C form with an initial state programmable to a maximum capacity of 5 A at 30 Vdc.

- aa) The integrated warning buzzer shall provide a sound level maximum of 85 dB.
 - bb) The two external power outputs shall provide 250 mA at 12 Vdc, be regulated, and have an electronic overload protection.
- 2) Card and Code Reader
- a) Physical Characteristics
 - (1) Mid-Range with Keypad Readers: Reader shall incorporate a standard 12-key digital keypad with the same numbering configuration as a standard touch-tone telephone.
 - (2) Mullion Readers: Reader shall have a width of less than 1.75 inches to mount without modification to narrow rail stile doors.
 - (3) Mid-Range Reader: Reader must be capable of providing a read range up to 6 inches without modification.
 - (4) Reader shall be potted with a UL Listed flame-retardant potting material.
 - (5) Reader cover shall be secured to the reader using a security screw.
 - (6) Reader shall be designed for both surface mounting and mounting on a single-gang electrical box.
 - (7) Reader shall operate in a temperature range -31 °F to 151 °F (-35 °C to 67 °C).
 - b) Performance Requirements
 - (1) Reader shall provide an operating distance of 1–6 inches depending on the reader model, card model, and mounting environment.
 - (2) Reader shall be capable of transmitting the card data in the Wiegand protocol.
 - (3) Reader shall operate across a voltage range of 8 – 16 Vdc.
 - (4) Reader shall operate at an average current not to exceed 130 mA DC, and it shall not exceed a peak of 260 mA DC for mid-range keypad units (100 mA DC average, 260 mA DC Peak for Mullion and Mid-Range units).
 - (5) Reader shall have a lifetime warranty against manufacturer defects and workmanship.
 - c) Proximity Cards
 - (1) The Wiegand cards shall be of either proximity or swipe type. They shall be sealed and resistant to normal usage and weather conditions. They shall be of ISO standard credit card size and thickness. They shall also be available in a key chain/key fob format.
 - (2) The cards shall not affect nor be affected by:
 - (a) Magnetically encoded cards such as credit cards or bankcards, even when stored side by side in a wallet.
 - (b) Coins, keys, or other metal parts.
 - (c) Shoplifting detections systems installed in certain retail outlets.
 - (d) Communication equipment.

- (e) Magnetic fields normally found in offices.
 - (3) It shall be impossible for a person who discovers a card to determine that the card belongs to a particular client.
 - (4) The access cards shall be guaranteed for a minimum period of two years from any defects resulting from normal use.
 - (5) The software shall electronically encode the cards so that their availability shall be restricted by the requirement of a particular site code.
 - (6) HID 125 KHz proximity cards of all standard formats, including Corporate 1000 and long format cards of up to 64 bits, shall be supported.
 - (7) XceedID 125KHz proximity cards of all standard formats shall be supported.
- 3) Numeric Keypad
- a) The numeric keypad is used for access control readers combining an access card and "PIN" code.
 - b) The numeric keypad shall meet or exceed the following specifications:
 - (1) Operate on a continuous low voltage of 12 Vdc.
 - (2) Solid construction and resistant to vandalism.
 - (3) LED indicator.
 - (4) Audible signal for each key touch.
- 4) Ethernet 32 I/O Device (for elevator integration)
- a) The Ethernet 32 I/O device shall be installed on the same subnet as the system management server.
 - b) The Ethernet 32 I/O device shall be configured with the system management system.
 - c) The Ethernet 32 I/O device shall contain 32 channels configurable as inputs or outputs.
 - d) When the Ethernet 32 I/O device channel is configured as an output can be configured as "normally open" or "normally closed". When configured as "normally closed, the output will provide a TTL level voltage (5 Vdc).
 - e) When I/O channels are configured as outputs, the device shall provide a combined current of at least 400 mA to connected devices.
- 5) Acceptable Manufacturer: Infinias, Inc. or Approved OEM [NO EXCEPTIONS]
- c. Secondary Components
- 1) Magnetic Contact: Recessed
- a) One recessed magnetic contact shall be installed on each door to be controlled or monitored. In locations where there are double doors, two contacts shall be installed and the connections shall be made so that the opening of each door is detected.
 - b) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install the recessed magnetic contacts per the following guidelines:
 - (1) The door contact shall be installed and centered on the upper doorframe, at a maximum distance of 4 inches from the opposite side of the door hinges.

- (2) The door contact shall be solidly anchored with adhesive or silicone so that it cannot be removed without breakage or the use of a special tool.
 - (3) When the contact is installed in the recessed part of a metal doorframe, an appropriate solidly attached metal support shall be used. The tolerance "gap" shall be adjusted to the frame and the door.
 - (4) The wiring shall optionally be supervised by an end-of-line resistor.
 - (5) A 0.50-inch conduit (or more as required) shall be supplied and installed between the door contact and the pull box to allow for connection to the duct network.
- 2) Magnetic Contact: Surface
- a) One or two surface magnetic contacts shall be installed on garage doors, gate barriers, and other entry points.
 - b) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install the surface magnetic contacts per the following guidelines:
 - (1) The contacts shall be solidly anchored using corrosion-resistant, tamper-resistant screws.
 - (2) Use of appropriate supports such as 0.25-inch steel plates (there should be no ground installations unless no other possibilities exist).
 - (3) The armored flexible cable supplied with the contact shall be solidly anchored to avoid being pulled out. It shall be connected to housing with tamper-resistant screws.
 - (4) In garage door installations, the contacts shall be arranged diagonally.
 - (5) The wiring shall (optionally) include an end-of-line resistor.
 - (6) A 0.50-inch conduit (or more as required) shall be supplied and installed between the door contact and the pull box to allow for connection to the duct network.
- 3) Electric Door Strike
- a) An electric door strike shall be installed on some single or double doors. It shall optionally be equipped with one micro-switch to supervise the presence and locking of the lock latch inside the door strike. The door latch shall be identifiable for monitoring, independently of other monitored components.
 - b) The security contractor shall confirm the compatibility of the strike with the type of door and hardware. Furthermore, when the door strike is installed on an exterior perimeter door, a security plate shall also protect this door.
 - c) The security contractor shall be held responsible for the malfunction of or damage caused to doors or doorframes as a result of the installation of door strikes or other devices.
 - d) When required (for a double door), the security contractor shall connect the electric door strike using a power transfer cable.
 - e) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install the electric door strike in compliance with the following guidelines:
 - (1) The wiring shall include an end-of-line resistor.
 - (2) A 0.50-inch (or more as required) conduit shall be supplied and installed between the electric door strike and the pull box to allow for connection to the duct network.
 - (3) The electric door strike shall operate on a continuous low voltage of

12 Vdc.

- 4) Electric Lock
 - a) The electric lock shall be installed on some doors to control the locking and unlocking of the doors (similar to an electric door strike).
 - b) The electric lock shall meet or exceed the following specifications:
 - (1) Operate on a continuous low voltage of 12 Vdc.
 - (2) Have a "fail secure" function.
 - (3) Be suitable for the existing type of door, doorframe, and hardware.
 - c) The security contractor shall be held responsible for the malfunction of or damage caused to doors or doorframes as a result of the installation of door locks or other devices.
- 5) Electric Panic Bar with Electric Lock
 - a) The security contractor shall take into consideration that this equipment may be supplied and installed by others, but he shall be responsible for the interconnections.
 - b) The security contractor shall foresee the power supply for the panic bars with an electric lock.
- 6) Monitoring Strike
 - a) Some doors shall be equipped with monitoring strikes for confirming the action of the strike.
 - b) The security contractor shall be held responsible for the malfunction of or damage caused to doors or doorframes as a result of the installation of door locks or other devices.
 - c) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install the monitoring door strike in compliance with the following guidelines:
 - (1) The wiring shall include an end-of-line resistor.
 - (2) The monitoring strike shall be identifiable for monitoring, independent of other monitored components.
 - (3) A 0.50-inch conduit (or more as required) shall be supplied and installed between the monitoring strike and the pull box to allow for connection to the duct network.
- 7) Power Transfer Cable
 - a) Power transfer cables shall be installed on some devices to ensure operation or power continuity.
 - b) The power transfer cable shall meet or exceed the following specifications:
 - (1) Hidden in the frame.
 - (2) Tolerate low voltage.
 - (3) Be adaptable to the type of hinge or door pivot.
- 8) Solenoid Switch
 - a) The security contractor shall supply a reliable solenoid switch system (dry contact with appropriate wiring) that shall interrupt the electric current to command buttons of the electric motors used for garage doors.
 - b) In the case of a turnstile or motorized door, the solenoid switch shall be used for the normal operation of the door, based on the delay required, to ensure the passage of persons or carts.

- c) In locations where additional appliances (such as chains or auxiliary pulleys) are necessary for the manual operation of the door during a power outage, the security contractor shall foresee a “dead bolt” mechanism that blocks the manual opening of the door disables the opening mechanism. These two actions shall be controllable from the control station.
 - d) The security contractor shall submit a diagram showing the operation of the solenoid switch to the general contractor for approval.
 - e) The solenoid switch shall be matched to the type of manual mechanism.
 - f) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install the solenoid switch using the following guidelines:
 - (1) A 0.50-inch conduit (or more as required) shall be supplied and installed between the solenoid switch and the pull box to allow for connection to the duct network.
- 9) Electromagnetic Lock
- a) An electromagnetic lock shall be installed to control some doors. The electromagnetic lock shall meet or exceed the following specifications:
 - (1) Holding force of 1,500 lbs.
 - (2) Two status light indicators (red and green) shall indicate the lock’s power and adequate holding force.
 - (3) Integrated contact switch to supervise the adequate holding force.
 - (4) The electromagnetic lock shall operate on a continuous low voltage of 12 Vdc.
 - b) In addition to the integrated contact switch supervising the holding force, the door shall be equipped with a recessed magnetic contact for supervising the door status.
 - c) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install the electromagnetic lock in compliance with the following guidelines:
 - (1) The electromagnetic lock shall be securely anchored on the upper doorframe with manufacturer-recommended security bolts.
 - (2) Connections of the electromagnetic locks shall allow monitoring of adequate holding force, independently of other components that require connection.
 - (3) The wiring shall include an end-of-line resistor.
 - (4) A 0.50-inch conduit (or more as required) shall be supplied and installed between the electromagnetic lock and the pull box to allow for connection to the duct network.
 - d) The security contractor shall be held responsible for the malfunction of or damage caused to doors or doorframes as a result of the installation of door locks or other devices.
 - e) All electromagnetic locks installed at emergency exits shall be connected to the panic bar controller or to a manual abort station, as required. The power supplies for the electromagnetic locks shall be connected to the building fire alarm system (supplied by a third party) to permit the de-activation of the electromagnetic locks in the event of a fire drill or a fire alarm.
 - f) The security contractor shall obtain authorization from local authorities before installing the devices. In addition, before final acceptance, he shall provide a written confirmation certifying that the installation has been executed per

- regulations.
- g) Signs indicating emergency procedures, that shall be located near each door equipped with electromagnetic locks, shall be supplied and installed by the general contractor and shall conform to applicable codes and regulations.
- 10) Electric Panic Bar with Timer
- a) A panic bar with electric contact, as well as control devices for panic bars, shall be installed on some doors designated as emergency exits in conformance of fire code regulations. In locations where a double door is installed, an additional panic bar shall be added.
 - b) The panic bars, control devices and the power transfer cables shall meet with or exceed the following specifications:
 - (1) Panic bar(s) equipped with an electric contact suitable for the door architecture.
 - (2) Electronic exit delay module with alarm contact and re-arming key switch including back box and accessories (two keys per cylinder).
 - (3) Wiring for delay activation monitoring (after 3 seconds) shall include an end-of-line resistor.
 - (4) Shall include an activation warning buzzer different than those on doors controlled with card readers or other devices.
 - (5) Embedded power transfer cables for panic bar connection.
 - (6) Signs indicating emergency procedures supplied and installed by the general contractor.
 - (7) Operation on a continuous low voltage of 12 Vdc.
 - (8) UL approved.
 - c) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall connect the panic bars and install the controls in compliance with the following guidelines:
 - (1) The panic bar control shall be concealed near the door.
 - (2) The warning buzzer for the panic bar control system shall be locally audible and sufficiently loud, taking into consideration background noise level.
 - (3) The re-arming key switch shall be connected so power can be restored to the electromagnetic lock, but it shall not permit the reverse operation.
 - (4) The warning buzzer location shall be chosen so that the buzzer can be heard in the targeted zone.
 - (5) The connection shall allow the power to electromagnetic lock to be removed in less than 15 seconds, or as required. The transmission of an alarm indicating that the power is removed is irreversible after 3 seconds.
 - (6) A 0.50-inch conduit (or more as required) shall be supplied and installed between the panic bar, the key switch, the panic bar control connection housing, the warning buzzer, and the pull box to allow for connection to the duct network.
 - (7) The security contractor shall be held responsible for the malfunction of or damage caused to doors or doorframes as a result of the installation of panic bars or other devices.
 - (8) The security contractor shall obtain authorization from local authorities before installing the devices. In addition, before final acceptance, he

shall provide a written confirmation certifying that the installation has been executed per regulation.

- (9) Signs indicating emergency procedures shall be located near each door equipped with electric panic bars. These signs shall be supplied and installed by the general contractor and shall conform to applicable codes and regulations.
- 11) Manual Abort Station
- a) A manual abort station shall be installed on some doors designated as emergency exits to conform to requirements in fire code regulations and any other recommendations.
 - b) The manual abort station shall meet or exceed the following specifications:
 - (1) The color shall be different from other manual fire pull stations.
 - (2) The housing shall be appropriate to the station for a surface or recessed installation.
 - (3) Signs indicating emergency procedures shall be supplied and installed by others.
 - (4) Double pull.
 - c) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall connect the manual abort stations in compliance with the following guidelines:
 - (1) The manual abort station shall be solidly anchored on the side opposite the door hinges.
 - (2) The connection shall allow the power to be removed from the electromagnetic lock and transmit an alarm indicating use of the manual abort station.
 - d) The security contractor shall obtain authorization from local authorities before installing the devices. In addition, before final acceptance, he shall provide a written confirmation certifying that the installation has been executed per regulation.
 - e) Signs indicating emergency procedures shall be supplied and installed near each door with a manual abort station by the general contractor. These signs shall conform to applicable codes and regulations.
- 12) Exit Request Devices
- a) There are two types of exit requests devices: an infrared sensor and a button. An exit request device provides a function equivalent to a reader, but without defining the user. A description of each device follows.
 - b) The infrared exit request device shall meet or exceed the following specifications:
 - (1) Operation on a continuous voltage of 12 Vdc.
 - (2) LED light indicator.
 - (3) Adjustable range area.
 - c) The exit request button device shall be installed on a strong aesthetic finishing plate.
 - d) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install exit request devices in compliance with the following guidelines:
 - (1) The wiring shall include an end-of-line resistor.

- (2) The device shall be suitable for the type of door or window where it is installed.
- (3) The location shall be chosen to deter involuntary or fraudulent activation.
- (4) A 0.50-inch conduit (or more as required) shall be supplied and installed between the exit request device and the pull box to allow for connection to the duct network.

13) Key Switch

- a) A key switch shall be used for the following purposes:
 - (1) A malfunction key switch allows the immediate or direct deactivation of an electromagnetic lock in the event of system failure. The key switch shall be equipped with a tamper contact that shall transmit an alarm to the monitoring station.
 - (2) An access key switch allows the temporary deactivation of the supervisory systems of a controlled door to permit access without generating an alarm (authorized access). The security contractor shall provide the electronic delay module and necessary accessories with the key switch. Where the key switch is used to open a motorized garage door, it shall be used with a command button panel (Open, Stop, Close) that can be used with limited time delays. This function shall also be available on a programmable schedule. When the key switch is used for door access authorization, it shall be determined whether it is an exit or an entry. It shall be possible to activate and deactivate the key switch based on a programmable schedule to authorize normal access without causing an intrusion alarm. The switch shall be equipped with a tamper contact that shall transmit an alarm to the monitoring station.
- b) The key switch shall be equipped with an LED to indicate the state of the function.
- c) The key switch shall meet or exceed the following specifications:
 - (1) Operate with a mortise cylinder with five pins.
 - (2) Two keys per cylinder.
 - (3) Momentary operation or other, as necessitated by the application.
 - (4) Illuminated with two status indicators (red and green lights), except for the fault interrupter.
 - (5) Aesthetic plate with security screws.
 - (6) Appropriate housing.
- d) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install key switch devices in compliance with the following guidelines:
 - (1) The device shall be installed on the side of the door opposite the hinges.
 - (2) The wiring shall include an end-of-line resistor.
 - (3) The key switch shall be equipped with a tamper contact that shall be connected independently so that the point of supervision can be distinguished from the use of the switch.
 - (4) A 0.50-inch conduit (or more as required) shall be supplied and installed between the key switch and the pull box to allow for connection to the duct network.

14) Man Trap

- a) When a man trap function is specified, the security contractor shall foresee all the necessary accessories to ensure and maintain the integrity of this function.
 - b) The security contractor shall show the general contractor that the operation of the man trap is compliant with the requirements.
- 15) Glass Break Detector
- a) The detection of glass breakage shall be suitable to the environment, of DOUBLE TECHNOLOGY type, and shall meet or exceed the following specifications:
 - (1) Shall provide detection at up to ± 9 yards
 - (2) Shall include a tamper switch
 - (3) Shall be illuminated with a LED display
 - (4) Shall operation on a voltage of 12 Vdc
 - (5) Shall include an alarm memory
 - (6) Shall have an adjustable sensitivity
 - b) The security contractor shall show the general contractor that the choice and number of devices meets the protection specifications, while not causing false alarms due to environmental factors or other equipment used by the general contractor.
 - c) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install glass break detectors in compliance with the following guidelines:
 - (1) The glass break detector shall ensure detection at a minimum height of 3 yards above ground level and accessible traffic areas.
 - (2) The glass break detector shall be securely anchored so it cannot be removed without breakage or the use of special tools.
 - (3) The glass break detector shall be equipped with a tamper contact connected separately to distinguish between an intrusion alarm and a tamper alarm.
 - (4) There shall be an option for clearing the alarm memory.
 - (5) The wiring shall include an end-of-line resistor.
 - (6) A 0.50-inch conduit (or more as required) shall be supplied and installed between the glass break detector and the pull box to allow for connection to the duct network.
- 16) Motion Detectors
- a) The motion detectors shall include a double technology (infrared / microwave sensor) and shall meet or exceed the following specifications:
 - (1) Shall include infrared and microwave supervision
 - (2) Shall include a tamper contact
 - (3) Shall include an illuminated LED display
 - (4) Shall effectively cover the required area, based on environment requirements. The detectors may be ceiling or wall mounted.
 - (5) Shall operate on a voltage of 12 Vdc.
 - b) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install motion detectors in compliance with the following guidelines:

- (1) The motion detector shall be installed and oriented so that the area of coverage meets with the general contractor's criteria.
 - (2) The motion detector shall be equipped with a tamper contact connected separately to distinguish between an intrusion alarm and a tamper alarm.
 - (3) The wiring shall include an end-of-line resistor.
 - (4) A 0.50-inch conduit (or more as required) shall be supplied and installed between the motion detector and the pull box to allow for connection to the duct network.
- 17) Strobe Lights
- a) A strobe light shall be installed near some emergency devices. The strobe light shall meet or exceed the following specifications:
 - (1) Shall operate on continuous voltage of 12 Vdc
 - (2) Shall have a clear color
 - (3) Shall have a pulsation frequency of 80 pulses per minute
 - (4) Shall be surface mounted on a ceiling
- 18) Siren Alarm
- a) A siren shall be installed near some emergency devices. The siren shall meet or exceed the following specifications:
 - (1) Shall operate on continuous voltage of 12 Vdc
 - (2) Shall consume at most 30 W power
 - (3) Shall emit a variable tone or pulsation
 - (4) Shall be mounted in a metal housing
- 19) Panic Switch
- a) The panic switch shall meet the following specifications:
 - (1) Shall be designed to avoid false alarms
 - (2) Shall be resettable with a key
 - b) Unless indicated otherwise, and taking into consideration the environment, the security contractor shall install panic switches in compliance with the following guidelines:
 - (1) The wiring shall include an end-of-line resistor.
 - (2) The device shall simultaneously transmit an alarm to the controller and to a panel for receiving and transmitting priority alarms.
 - (3) The device shall be hidden and easily accessible when it is installed at a workstation.
 - (4) The location of the device shall be coordinated with the general contractor based on the operations.
- 20) Interior Turnstile
- a) An interior turnstile (supplied and installed by others in designated areas) shall meet the following specifications:
 - (1) Shall operate on a voltage of 110 Vac with low voltage control.
 - (2) Shall operate in two directions with a "fail secure" option.
 - (3) Shall operate with card readers and by remote control.
 - b) The security contractor is responsible for integrating equipment such as card

readers and ensuring the local and remote operation.

21) Traffic Gate

- a) The traffic gate shall meet the following specifications:
 - (1) Shall operate on a voltage of 110 VAC with low voltage control.
 - (2) Shall operate with card readers and remote control.
 - (3) Shall operate with a remote control with two buttons (Open, Close).
 - (4) Shall include a protection buckle and automatic closure in the cement slab.
- b) The traffic gate implementation shall be submitted for approval.
- c) The security contractor shall be responsible for supervising the condition of the gates and ensuring the local and remote operation.

22) Electric Door Controller

- a) An electric door controller shall be installed on some doors to open or close them automatically. The door controller shall meet or exceed the following specifications:
 - (1) Shall operate on a voltage of 110 VAC with low voltage control.
 - (2) Shall be suitable for the type of door and frame.
 - (3) Shall be surface mounted.
 - (4) Shall permit opening the door with a swing range of 110–130 degrees.

23) Door Stop

- a) The security contractor shall make connections to certain devices to activate the closure, on demand, of certain emergency doors.
- b) The power source to the doorstops shall be disabled to activate the automatic closure of the doors.

d. Control Station

1) Computers: Server and Workstation

- a) The server shall process and record all the data acquired by the access controllers.
- b) The system shall function without the server being logged onto.
- c) The server software shall be fully operable in a virtual environment such as VMWare ESXi or higher.
- d) The workstation software shall be browser based and shall not require ActiveX or other plug-in. The software shall be written using only HTML and JavaScript language.
- e) There shall be no installation required at the workstation. The user will run the software by browsing the server with an industry standard browser.
- f) The system will support the most recent releases of Microsoft Internet Explorer, Google Chrome and Mozilla Firefox at a minimum.
- g) The primary computer shall be equipped with the following minimum requirements:
 - (1) Windows® XP Professional (with Service Pack 2)
 - (2) Processor at 2 GHz or faster
 - (3) 2GB RAM
 - (4) 120GB hard disk

- (5) 1 USB port (or additional parallel port for badging)
 - (6) 19-inch, 1280 x 1024 true color monitor
 - (7) Standard keyboard
 - (8) Standard mouse
 - (9) Network Interface Card (NIC)
 - h) The secondary computer shall be capable of normal internet browsing.
 - i) The computers shall be capable of communicating with numerous access controllers, terminals, or other computers in a multitasking/multi-usage mode or network mode.
4. Communication Network and Cable
- a. Cabling Conduits
 - 1) The general contractor shall supply and the security contractor shall install the primary and secondary conduits in compliance with the following specifications:
 - a) In the event that the power voltage is superior to 48 V or a hazardous condition exists, the following shall be completed.
 - b) The wiring shall not be hidden in the divisions or the walls.
 - c) All conditions shall be subject to codes or norms in force.
 - d) If there are visible conduits, it shall be possible to use surface conduits. An authorization to do so shall be obtained prior to installation.
 - e) The use of flexible conduits shall be authorized in the case of descent into a division or in areas that are difficult to access.
 - f) The sizing of the conduits shall respect a maximum fill of 40%.
 - g) The general contractor shall use cable paths or designated spaces for cable passage.
 - 2) The security contractor shall coordinate the planning and installation of the conduits with the general contractor.
 - 3) The security contractor shall verify that the size of the conduits meets the aforementioned requirements and is compatible with the needs. The security contractor shall present any conduit network modifications and adjustments to the general contractor for approval prior to installation.
 - b. Cables
 - 1) The general contractor shall supply and the security contractor shall install the power cables, control cables, and other cables for the primary and secondary networks.
 - 2) All wires, cables, and connectors shall bear the same identification number at both ends.
 - 3) The cabling required for the readers shall be 6 conductors, 22 gauge.
 - 4) If the use of a terminal block is required, the cables shall be equipped with a fork connector or ring.
 - 5) All spliced connections shall be soldered and indicated on the mechanical plan before soldering. Splices shall be covered with shrink tubing.
 - 6) Cables in housings shall be securely attached with "tie wrap" bindings.
 - 7) All cables used for the installation shall meet the manufacturer recommendations.
 - c. Equipment Supplied by Others
 - 1) Some specific equipment may be provided and installed by other contractors. The

security contractor is responsible for the coordination of his work with that of the other contractors. The security contractor is responsible for the interconnection and shall test the operation of all equipment with that installed by other contractors.