SECTION 28 13 00 – ACCESS CONTROL

1. PART 1 GENERAL
   1. RELATED DOCUMENTS
      1. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.
      2. Divisions 26, 27, and 28 basic materials and methods sections apply to work specified in this section.
   2. SUMMARY
      1. This Section includes an IP based security access control system (ACS) consisting of a Cloud Host Service, client workstations utilizing any supported web browser and field-installed IP based Reader-Controllers and/or IP-Bridges connected by a high-speed electronic data transmission network. This system’s features include regulating access through controlled openings, credential management, monitoring of field devices, and reporting.
      2. Related Sections:
         1. 14 28 16 – Elevator Controls
         2. 28 16 33.16 – Intrusion Detection Interfaces to Access Control Hardware
         3. 28 16 43 – Perimeter Security Systems
         4. 26 05 53 – Cabling, Conduit, and Junction Box requirements
         5. 27 15 00 Category and/or Optical Fiber Cable and connectivity specification and installation standards
         6. 08 17 00 – Door Hardware
   3. REFERENCES
      1. Abbreviations and Acronyms
         1. ACS – Access Control System
         2. AES – Advanced Encryption Standard
         3. I/O – Input/Output
         4. ISAM – Indexed Sequential Access Method
         5. LAN – Local area network.
         6. LED – Light-emitting diode
         7. PC – Personal Computer
         8. RFID – Radio Frequency Identification
         9. TCP/IP – Transport Control Protocol/Internet Protocol
         10. UPS – Uninterruptible power supply.
         11. WAN – Wide area network
      2. Definitions
         1. ACS Cloud Service – A cloud based service hosted and maintained by the Manufacturer for administrating and communicating to Reader Controllers and IP-Bridges.
         2. IP based Reader-Controller - An intelligent network-connected reader controller unit with inputs, outputs and data storage capability.
         3. IP-Bridge – An intelligent interface to legacy based access control systems using traditional structured cabling and proximity readers.
         4. Access Point – Any Reader Controller or port on an IP-Bridge connected to the ACS Host.
         5. Credential - RFID based token assigned to an entity and used to identify that entity.
         6. Mobile Credential – Token using Bluetooth® Low Energy on any Android or Apple device
         7. Identifier - A credential card, keypad personal identification number or code, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual. Where this term is presented with an initial capital letter, this definition applies.
         8. RFID - An automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders.
         9. Client - Any device with a supported web browser that can connect to either the Cloud Service or Host Server.
      3. Reference Standards
         1. SIA BIO-01-1993.02(R2000.06) - Biometric Standard - Vocabulary for Testing
         2. Institute of Electronic and Electrical Engineers (IEEE) 802.3 standards
         3. Underwriters Laboratories
            1. UL 294 - Access Control System Units
            2. UL 294B - Power Over Ethernet
         4. FCC 47, CFR Part 15
         5. Industry Canada - Radio Standards Specification RSS-210 License-exempt Radio Apparatus
         6. National Institute of Standards and Technology (NIST)
            1. FIPS 197 - Advanced Encryption Standard (AES)
         7. ISO 14443A, 14443B - Proximity Cards
         8. EIA/TIA-569 - Commercial Building Standard for Telecommunications Pathways and Spaces
         9. ETSI EN300, EN330-2, EN301 489-1
   4. SUBMITTALS
      1. General:
         1. Submit in accordance with Conditions of Contract and Division 01 requirements.
         2. Highlight, encircle, or otherwise specifically identify on submittals deviations from Contract Documents, issues of incompatibility or other issues which may detrimentally affect the Work.
         3. Prior to forwarding submittal, comply with procedures for verifying existing door and frame compatibility for new hardware, as specified in PART 3, “EXAMINATION” article, herein.
      2. Action Submittals
         1. Product Data
            1. Manufacturers’ printed and electronic data sheets, including operating characteristics, furnished specialties, and accessories.
            2. References for each product to a location on Drawings.
            3. Test and evaluation data presented in compliance with SIA BIO-01
            4. Manufacturers’ installation and operation manuals
         2. Shop Drawings
            1. Diagrams for cable management system.
            2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Part 2.
            3. Wiring Diagrams. Show typical wiring schematics including the following:

Workstation outlets, jacks, and jack assemblies.

Patch cords.

Patch panels.

Active network components.

* + - 1. System installation planning documents
    1. Closeout Submittals
       1. Field quality-control test reports
       2. End User Training Plan
       3. Operation and Maintenance Data
          1. Microsoft Windows software documentation.
          2. For each PC, installation and operating documentation, manuals, and software for the PC and all installed peripherals.

Include system restore, emergency boot diskettes, and drivers for all installed hardware.

The software manual shall describe the functions of all software and shall include all other information necessary to enable proper programming and operation. The manual shall fully explain all procedures and instructions for the operation of the system.

* + - * 1. System installation and setup guides.
      1. List of recommended spare parts. Insert a list of spare parts, or delete
  1. QUALITY ASSURANCE
     1. Electrified Door Hardware: Listed and labeled as defined in NFPA 70, Article 100, by testing agency acceptable to authorities having jurisdiction.
     2. Coordination Conferences:
        1. Electrified Hardware Coordination Conference: Prior to ordering electrified hardware, schedule and hold meeting to coordinate door hardware with security, electrical, doors and frames, and other related suppliers.
     3. Installation Contractor:
        1. Integrating firm shall have worked satisfactorily for a minimum of (5) years of completing systems equal to this scope, quality, type and complexity.
        2. Key personnel assigned to the project shall each have a minimum of (5) years of experience in completing systems equal to this scope, quality, type and complexity.
        3. Contractor shall maintain complete installation and service facilities for the duration of the project contract.
     4. All work shall be done by expert technicians qualified in the field with knowledge of specified systems. Workmanship shall comply with industry best practices concerning grounding, shielding, cable dressing, cable termination and equipment mounting.
     5. Where required by the local municipality, technicians are required to have proper licensing to perform work within this specification.
  2. DELIVERY, STORAGE, AND HANDLING
     1. IP Bridges and IP-based Reader-Controllers:
        1. Store in temperature and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between -40 and 120 deg F (-40 and 50 deg C).
        2. Open each container; verify contents against packing list, and file copy of packing list, complete with container identification for inclusion in operation and maintenance data.
        3. Mark packing list with designations that have been assigned to materials and equipment.
  3. COORDINATION
     1. Security: Coordinate installation of door hardware, keying, and access control with Owner's security consultant.
     2. Coordinate with Owner, Division 08 contractor, and electrical contractor prior to rough-in to coordinate exact location of end devices and door functionality.
     3. Electrical System Roughing-In: Coordinate layout and installation of electrified door hardware with connections to power supplies and building safety and security systems.
     4. Meet at least once, prior to rough-in, with horizontal cabling installer to verify all cabling requirements. Coordinate cable jacketing color according to specification 25 05 53. *Remove this item if cabling is being provided by the security contractor, and not a structured cabling company.*
     5. Division 26, 27, and 28 contractors shall verify electrical service provided prior to ordering any electrical equipment serving electronic door hardware equipment, and maintain responsibility for properly coordinating the electrical work including location of the electrical connections.
     6. Obtain submittals of all door hardware equipment from door hardware specification and Division 08. Carefully review door hardware submittal and advise in writing of any discrepancies through an RFI.
     7. The contractor shall include necessary wiring and programming for fire-alarm panel tie-in and door release based upon the requirements and direction of the Owner and/or AHJ. Contractor is responsible to schedule and coordinate with fire alarm contractor.
     8. Coordinate all interfaces between door hardware and electrical contractor.
     9. A licensed and insured Electrical Contractor shall provide 120VAC power to all locations requiring power. *Modify as needed, based on power requirements of door hardware and/or IP Bridges.*
  4. warranty
     1. Security Integrator shall provide a limited one year hardware warranty for the product to be free of defects in material and workmanship.
     2. Security Integrator shall provide software updates for cloud service as they are available and will be automatically granted. On premise software updates are available through a software upgrade program.
     3. Manufacturer shall make available an extended warranty and maintenance support option.

1. PART 2 PRODUCTS
   1. EQUIPMENT
      1. Authorized Manufacturer(s): Schlage
      2. Models:
         1. Software: Pure Access™ Cloud
         2. Hardware:
            1. IP Reader Controller
            2. IP Bridge
            3. NDEB wireless electronic lockset
            4. LEB wireless electronic mortise lockset *Remove any components above that will not be utilized on this project.*
      3. Acceptable Manufacturers: No Substitution.
   2. DESCRIPTION
      1. Provide a complete and operational access control system (ACS) as indicated in the drawings and plans, including but not limited to an ACS Cloud Service Host, IP based Reader-Controllers and/or IP-Bridges connected by a high-speed electronic data transmission network.
         1. The Cloud Service shall be host on Amazon Web Services and provide for a minimum of 99.95% uptime. The Manufacturer shall closely monitor all conditions related to the Cloud Service infrastructure.
      2. The network connecting the ACS Cloud Service Host, IP Bridge and IP based Reader-Controllers shall be a Local Area Network (LAN) or Wide Area Network (WAN) utilizing TCP/IP communications protocol.
      3. Functions - The systems primary functions shall include
         1. Regulating access through doors, gates, turnstiles, and other entrance portals
         2. Credential cards and readers
         3. Credential creation and credential holder database and management
         4. Monitoring of field-installed devices
         5. Reporting
      4. Third Party Devices - In addition to supporting the Manufacturer’s own multi-card readers, the system shall support the following types of readers by utilization of an IP Bridge:
         1. Wiegand output devices including but not limited to:
            1. Biometric devices
            2. Long Range Readers such as Tagmaster
            3. Barcode scanners
   3. SYSTEM SOFTWARE
      1. The ACS Host application software shall provide the interface between the Client, IP-Bridges, IP based Reader-Controllers, report alarms, generate reports and provide all other system functions.
      2. The system shall provide a web based User Interface using standard browsers such as Chrome, Firefox and Microsoft Edge. Mobile devices such as tablets and smart phones will be able to log in via the same such browsers and have a User Interface optimized for mobile experience.
      3. The system software license shall be licensed as follows:
         1. ACS Cloud Service
            1. License shall be provided for the desired number of access points and users.
            2. Shall be an annual fee paid to maintain the Cloud Service and provide regular updates.
      4. System Functions - The access control system software functions shall include the following:
         1. User/Credential Management
            1. Number of users and credentials dependent upon license limitations.
            2. User group functionality
            3. Users configuration shall have the following attributes:

First name, middle initial, and last name.

User Image

Alert email address for the User to receive Alert emails

Ten (10) customizable User Defined Fields

Web Access with customizable User Roles to define what the User can view and edit in the Client. Passwords for Web Access shall be forced to use strong passwords.

Can reside in an unlimited number of User Groups.

Can be associated with Custom Rules

* + - * 1. When deactivating a User, the system shall deactivate all associated credentials with that User. Any credential can be deactivated without deactivating the associated User.
        2. Microsoft Active Directory Integration

System shall allow for the integration to Microsoft Active Directory unless it is utilizing a Cloud Service license of under fifty (50) Access points. This Integration will synchronize Users from Active Directory to the ACS Host. The ACS Host will poll the Active Directory server regularly for changes and synchronize those changes to its database.

* + - 1. Access Point Programming and Management
         1. Provide an easy to use wizard to add Access points to the software
         2. Wizard shall include a full test of all Access Point components
         3. Configurable door latch interval
         4. Input enable/disable and configuration
         5. Number of Access Point Groups - Unlimited
      2. Weekly Schedules
         1. Number of Weekly Schedules - Unlimited
         2. Interval assignments - Any day of the week
      3. Weekly Rules configurable based on type of device being used
      4. Alarm and Event Logging - provide for logging of all system alarms and events chronologically including time and date stamp. Specific alarm conditions monitored shall be included but not limited to:
         1. Door Unauthorized Open Alarm
         2. Door Extended Open Alarm
         3. Reader-Controller Tamper Alarm
         4. Device Offline Alert
      5. System Scheduling - provide for scheduling of events including:
         1. Access Point or Access Point Group unlock for specified Schedule.
         2. Access Point or Access Point Group unlock with specified Badge(s), Access Point(s) shall remain locked until an authorized Credential is read.
      6. System Dashboards – Monitoring Attributes
         1. Shall provide customizable Dashboards for Monitoring of the ACS. These Dashboards shall be fully customizable, able to filter on all events, able to filter on all devices where applicable and include the following:

Ability to display non-wireless single Access Point status with the following:

Live update of door status including physical door status and all event history on devices connected in real-time.

Ability to Admit entry for the latch interval time

Ability to Admit, Unlock and Lockdown the Access Point

Display User images if available

Ability to display multiple Access Points, up to twelve (12) in a single widget with the following:

Live update of door status

Ability to Admit entry for the latch interval time

Ability to Lock, Unlock and Lockdown the Access Point connected to the Reader Controllers

Ability to display History in the system filtered to be filtered by Users, Groups and/or Access Points.

Ability to add a single Admit widget for an Access Point to admit entry for the latch interval.

Ability to add a Lockdown widget to Lockdown a single Access Point, a Group of Access Points or All Access Points.

Ability to show User profiles for a single Access Point or multiple Access Points. The User Profile shall show the event and Users image if applicable.

* + - * 1. Dashboards shall be able to be restricted by User Groups and/or Areas.
      1. System Alerts – Alarm Attributes
         1. System shall provide a dedicated page for monitoring of Alerts in the system. These alerts shall notify the User of the number of Alerts in the system and can easily configure email and/or SMS alerts to notify Users.
         2. Alerts shall queue in the system until they are Acknowledged and Cleared.
         3. Alerts shall be able to be Disabled or set to Auto-Clear from the queue.
         4. The types of Alerts available shall be:

Unauthorized Open

Extended Open

Tamper

AUX

REX

Credential Rejected

Credential Expired

Credential Over Limit

* + - 1. Reports
         1. System shall provide both customizable ad hoc reporting and scheduled reports that can be emailed on a daily or weekly basis.
         2. Reports shall be able to be saved as standard PDF or CSV files.
         3. Reports shall be able to be filtered by attributes within the report.
         4. The following reports should be included at a minimum:

History

Users

Access Points

Schedules

Attendance

Permissions

* + - 1. Custom Rules Engine
         1. System shall provide a flexible Custom Rules Engine to trigger unique actions from various events in the system. The Engine shall allow for the use of multiple triggers in the system to configure these events. System triggers shall include but not be limited to:

A User’s Credential is Accepted or Rejected

An Access Point has a specific Alert or any Alert

The Access Point has disconnected

During or not during a configured Schedule

At an Access Point or Access Point Group

* + - * 1. System Actions shall include but not be limited to:

Email a User or User Group

Lockdown an Access Point or Access Point Group

Create an Alert in the system

Unlock an Access Point or Access Point Group

Disable a Credential

* 1. HARDWARE COMPONENTS
     1. Field Devices and Functionality
        1. Field equipment shall include IP based Reader-Controllers and IP-Bridges. Wireless electronic locksets shall also be utilized. *Delete previous sentence if wireless electronics locksets are not used on this project (NDEB and/or LEB)*
        2. Data exchange between the ACS Cloud Host and the IP based Reader-Controllers shall include down-line transmission of commands, software, and databases to IP based Reader-Controllers.
        3. The up-line data exchange from the IP based Reader-Controller to the ACS Cloud Host shall include status data such as status reports, and entry-control records.
     2. Multi-technology IP Reader-Controller:
        1. Manufacturer: Schlage
           1. RC11 mullion mount
           2. RC15 single gang mount
           3. RCK15 single gang mount with keypad
        2. Credentials: The wireless locks shall provide credential reader modules in the following configurations, as indicated in door hardware sets:
           1. 125 kHz contactless proximity credentials with a bit format compatible with the electronic lockset

Compatibility: prox FSK and ASK such as Schlage, ISONAS, HID, GE/CASI ProxLite, AWID, LenelProx

* + - * 1. 13.56 MHz contactless smart cards

Secure section (multi-technology and smart card) compatibility: MIFARE Classic, MIFARE Plus, MIFARE DESFire

* + - * 1. Mobile Credential Model

2.4 GHz Bluetooth Low Energy Schlage mobile credential

* + - 1. Stand-alone Capability
         1. 64,000 credentials
         2. 5000 stored access events
         3. 32 schedules per credential
      2. Input/output
         1. Inputs - Three configurable (Default usage - door sense, request for exit/auxiliary)
         2. Outputs

One solid state relay controlling the electric lock rated at 12vdc 600ma.

* + - 1. Communications Interface
         1. Ethernet, TCP/IP via RJ-45 connector.
         2. Non-polled asynchronous messaging.
      2. Security
         1. TLS version 1.2 encryption
         2. Tamper detection via accelerometer
         3. Encrypted lock control with optional module
      3. Electrical
         1. Power – 12 VDC, PoE, PoE+
         2. Operating Current – 210-225mA peak
         3. Auxiliary Power Output – 12 VDC @ 600mA
      4. User
         1. LED Indicators (3) - reader status, network connection
         2. Programming - Microcode flash upgradeable
         3. Dual-mode reset button - Power-cycle reader and Reset-to-Factory defaults
      5. Physical and Environmental
         1. Operating Temperature - -40º to +66º C
         2. Humidity - 0 - 100%
         3. Weather Resistance – Conformal Coated components for weather resistance
         4. Certifications

UL-294 V7 Compliant

FCC 47 CFR Part 15

IC Certification

cUL Listed

RED Directive

CE Mark

IP65

REACH

Bluetooth SIG

RoHS 3

* + - 1. Enclosure

Durable U/V stabilized, flame-retardant ABS

Form Factor: Wall mount and mullion mount

Dimensions:

Mullion (5.94” x 1.77” x 1”)

Wall mount (5.13” x 3.25” x 1”)

* + - 1. Accessories
         1. Provide pigtail cable to connect the reader controller to the locking device and other accessories around the door.
         2. Provide Advanced Security Module at all reader controllers.
    1. Wireless Electronic Locksets: *Delete Wireless Electronic Lockset section if NDEb and/or LEb are not being used on this project.*
       1. Manufacturer: Schlage Select NDEB or LEB below, as required for the project.
          1. NDEB Cylindrical lockset compatible with 1-5/8 to 2 inch (41-51mm) doors with a 2-3/4 inch backset (2-3/8 inch optional). Latch bolt shall be 1/2 inch (12mm) throw steel dead-latching. For fire rated double (pair) doors, an optional 3/4 inch (19mm) throw steel anti-friction deadlatch shall be provided. Levers shall be pressure cast zinc, in a design and plated finish to match the mechanical locksets specified in 087100 Door Hardware.
          2. LEB Mortise lockset standard A115.1 preparation for 1-3/4 inch (44mm) doors. Options available for 2-1/4 inch doors. Backset shall be 2-3/4 inches, with a 3/4 inch (19mm) throw stainless steel latch bolt with anti-friction tongue. Optional 1 inch throw stainless steel deadbolt available with certain functions. Levers shall be made of forged brass or bronze and operate independently of each other. Lever design shall match the mechanical locksets specified in 087100 Door Hardware.
       2. Lockset shall combine lock, credential reader, door position sensor, and request-to-exit switch in a single unit, with the ability to be set up and configured wirelessly with a connected smartphone or tablet.
       3. Lockset shall provide an emergency key over-ride.
          1. Coordinate cylinder and keying requirements with 087100 Door Hardware.
       4. Lockset shall employ Wi-Fi communications for configuration and control of lock settings and users permitting remote view of audits and alerts, and configurable time period for updates.
       5. Encryption Keys
          1. Schlage default encryption key
          2. Schlage custom encryption key service (SCEKS)
       6. Credentials: The wireless locks shall provide credential reader modules in the following configurations, as indicated in door hardware sets:
          1. 125 kHz contactless proximity credentials with a bit format compatible with the electronic lockset

Compatibility: prox FSK and ASK such as Schlage, ISONAS, HID, GE/CASI ProxLite, AWID, LenelProx

* + - * 1. 13.56 MHz contactless smart cards

Secure section (multi-technology and smart card) compatibility: MIFARE Classic, MIFARE Plus, MIFARE DESFire

* + - * 1. Mobile Credential Model

2.4 GHz Bluetooth Low Energy Schlage mobile credential

* + - 1. Records: Subject to the limitations of the access control system, the wireless locks shall possess sufficient storage capacity to support 5000 credentials and 2000 audits.
      2. Performance: Credential verification time shall be less than or equal to one (1) second with smart cards and proximity cards.
      3. Third-party compatibility:
         1. The wireless locks shall employ an open architecture supportive of existing access control technologies and adaptable for future technologies.
         2. Cloud-based and mobile apps shall be supported without the need for an integrated software partner.
      4. Wireless communications
         1. Wi-Fi

Frequency: 2.4 GHz per IEEE802.11b/g/n

Wireless security: IEEE 802.1x, WPA2, WPA, WEP

Data Rate: 54 Mbps

* + - * 1. Bluetooth Low Energy: Version 4.2
        2. Communications security: Transport Layer Security (TLS) v1.2
        3. Encryption: Advanced Encryption Standard (AES) 256 bit
      1. Status Parameters and Indicators
         1. Via remote communication:

REX

door position

interior cover tamper

magnetic tamper

lock/unlock status

communication status

* + - * 1. Visual: LED (red, amber, green)
        2. Audible: Configurable and capable of being enabled or disabled C
        3. Power: 4 x 1.5V AA Batteries
        4. Wireless locks shall have the ability to communicate battery status and battery voltage level by means of an application on mobile device, at the door, and remotely by integrated software.
        5. Battery life: up to 2 years
      1. Mechanical additional characteristics:
         1. Tamper-resistant screw: torx screw on inside battery cover.
         2. Switch inputs:

door position switch

interior cover tamper

Request to Exit (REX)

* + - * 1. Available options:

interior push button

* + - 1. Environmental
         1. Operating Temperature:

Exterior: -31° to 151°F (-35° to 66°C)

Interior: 32° to 120°F (0° to 49°C)

* + - * 1. Humidity: 0 - 100% non-condensing
    1. IP Bridge: The system shall have available an IP-Bridge module to interface existing analog or IP access control equipment to the access control system specified herein over the IP network.
       1. The IP Bridge shall have the capacity to interface to up to three (3) doors.
          1. The IP Bridge shall have two (2) RJ-45 network connections, allowing connection of up to five (5) IP-Bridges to a single network switch port.

*NOTE: Consult factory for power considerations when interconnecting multiple IP Bridges. 12VDC is recommended for IP Bridges beyond the first.*

* + - 1. The IP Bridge shall eliminate the need for a stand-alone door controller with a capacity of:
         1. 20,000 cardholders
         2. 5000 access events
         3. 32 time zones per cardholder
      2. The IP Bridge shall have the ability to be configured and accessed by the ACS Host software.
         1. Information shall be exchanged on an asynchronous interrupt basis without the need for polling by the ACS Host software.
         2. IP Bridge microcode updates shall be provided over the network, when necessary.
      3. The IP Bridge shall support AES encryption.
      4. The IP Bridge shall have the ability to function autonomously in a Stand-Alone mode to reduce network traffic and system load.
      5. The IP Bridge shall support the following inputs (per access point):
         1. Three (3) configurable sensor inputs for door sense, request to exit and auxiliary.
         2. Wiegand card reader connection up to 1000 feet using 18/2 wire.

*NOTE: The three sensor inputs are typically used for door sense (normally closed), request for exit (REX, normally open) and an optional input for flexibility (AUX, normally open).*

* + - 1. The IP Bridge shall support the following outputs (per access point):
         1. Door Control relay (for electric lock, rated 2.0 A @ 30 VDC, form C)
         2. Wiegand interface

Power - 10 VDC regulated, regardless of input power to IP Bridge

LED control

beeper control

* + - * 1. Auxiliary 12 VDC power

*NOTE: The POE+ version of its IP-Bridge product supports 19 watts (1.6 A @ 12 VDC) power output.*

* + - 1. The IP Bridge shall have the capability to be powered by IEEE 802.3af POE, IEEE 802.3at POE+, or by 12 or 24 VDC
      2. User
         1. Indicators

Power

Network Status

Door Status (one indicator per door)

* + - * 1. Programming - Microcode flash upgradeable
        2. Dual-mode reset button - Power-cycle IP-Bridge and Reset-to-Factory defaults
      1. Physical and Environmental
         1. Operating Temperature - -40º to +50º C
         2. Humidity - 0 - 90%, non-condensing
         3. Enclosure

PC/ABS Flame-retardant per UL94 V-0

Form Factor - DIN Rail Mounting

Dimensions – 6.3” x3.6” x 2.3”

* 1. SYSTEM PERFORMANCE
     1. The system shall use a single database for access-control and credential-creation functions.
     2. Distributed Processing - The system shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to the IP based Reader/Controllers so that each IP based Reader-Controller can make access-control decisions for that location. If communications to ACS Host Workstation is lost, all IP based Reader-Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall automatically be uploaded to the ACS Host.
     3. System Response to Alarms
        1. Reader-Controllers network shall provide a system end-to-end response time of 3 second or less for every device connected to the system with typical network latency.
        2. Alarm and status changes shall be displayed within 3 seconds after receipt of data by the ACS Host with typical network latency.
        3. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within 15 seconds of alarm receipt at the security console with typical network latency.
     4. Network
        1. The TCP/IP network interconnecting the system components shall provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
        2. Network communication issues shall not require operator initiation or response, and the network shall return to normal after partial or total network interruption such as power loss or transient upset.
        3. Data Line Supervision - The system shall monitor the status of the data transmission lines with the use of heartbeat messages. The loss of the heartbeat messages will cause an alarm condition within the ACS host, and the reader-controller to switch to standalone mode.
     5. Environmental - The system shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:
        1. Exterior locations: Shall function as intended at the test voltage with its related equipment at ambient temperatures of minus 35 and plus 66 degrees C (minus 31 and plus 151 degrees F). The exposure to each of the temperatures is to be four hours or more.

1. PART 3 EXECUTION
   1. EXAMINATION
      1. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.
      2. Examine roughing-in for LAN and control cable conduit systems to PCs, IP based Reader-Controllers, Reader-controllers, non-IP readers, doors, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.
      3. Proceed with installation only after unsatisfactory conditions have been corrected.
   2. PREPARATION
      1. Comply with recommendations in SIA CP-01.
      2. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."
      3. Develop Project planning forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.
         1. Record setup data for control station and workstations.
         2. For each Location, record setup of IP based Reader-Controller features and access requirements.
         3. Propose start and stop times for shifts and holidays, and match up permissions for doors.
         4. Set up groups, and list inputs and outputs for each IP based Reader-Controller.
         5. Prepare and install alarm graphic maps.
         6. Discuss badge layout options; design badges.
         7. Complete system diagnostics and operation verification.
         8. Prepare a specific plan for system testing, startup, and demonstration.
         9. Develop acceptance test concept and, on approval, develop specifics of the test.
      4. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.
   3. CABLING
      1. Comply with NECA 1, "Good Workmanship in Electrical Contracting."
      2. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."
      3. Wiring Method: Install wiring in raceway except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.
      4. Wiring Method: Install LAN cables using techniques, practices, and methods that are consistent with Category 5e or Category 6 rating of components and that ensure Category 5e or Category 6 performance of completed and linked signal paths, end to end.
      5. Install cables without damaging conductors, shield, or jacket.
      6. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.
   4. CABLE APPLICATION
      1. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."
      2. Cable application and requirements shall be compliant with manufacturer’s recommendations.
   5. GROUNDING
      1. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."
      2. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."
      3. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.
      4. Bond shields and drain conductors to ground at only one point in each circuit.
   6. IDENTIFICATION
      1. In addition to requirements in this Article, comply with applicable requirements in Division 26 Section "Identification for Electrical Systems" and with TIA/EIA-606.
      2. Label each terminal strip and screw terminal in each cabinet, rack, or panel.
         1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the device as shown.
         2. Each wire connected to building-mounted devices shall be numbered at the device and shall be consistent with the associated wire connected and numbered within the panel or cabinet
   7. INSTALLATION
      1. Install all equipment in accordance with the manufacturer’s installation manuals, wiring diagrams and recommendations.
      2. Install, configure and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner.
      3. Testing: Upon completion of installation of system and after energized, demonstrate system compliance with intent.
   8. FIELD QUALITY CONTROL
      1. Contractor shall inspect, test, and adjust components and equipment installation.
         1. Results shall be reported in writing.
      2. Contractor shall perform the following field tests and inspections and prepare test reports:
         1. LAN Cable Procedures - Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
         2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
         3. Operational Test - After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.
      3. Contractor shall remove and replace malfunctioning devices and circuits and retest as specified above.
   9. STARTUP SERVICE
      * 1. Provide a fully commissioned system to ensure the entire system is operating as intended.
        2. Include any necessary programming for fire-alarm panel tie-in and door release based upon the requirements and direction of the owner and/or AHJ.
        3. Coordinate with the Owner and input all users, user groups, and schedules.
      1. Provide training on the operation and maintenance of the security access system.
         1. Representative shall develop separate training modules for the following:
            1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software
            2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel
            3. Security personnel
            4. Hardware maintenance personnel
            5. Corporate management

END OF SECTION