SECTION 28 13 00

ACCESS CONTROL

PART 1 - GENERAL

1.01 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.02 SUMMARY

A. Section Includes:

1. Access Control system installation and configuration.
2. Integration with a campus wide existing S2 head-end server.
3. Field Devices (Card Readers, Request to Exits, Door Contacts, etc.).

1.03 DEFINITIONS

A. CCTV: Closed-circuit television.

B. CPU: Central processing unit.

C. Credential: Data assigned to an entity and used to identify that entity.

D. Identifier: A credential card; keypad personal identification number; or code, biometric characteristic, 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.

E. I/O: Input/Output.

F. LAN: Local area network.

G. Location: A Location on the network having a PC-to-controller communications link, with additional controllers at the Location connected to the PC-to-controller link with a TIA 485-A communications loop. Where this term is presented with an initial capital letter, this definition applies.

H. PC: Personal computer.

I. PCI Bus: Peripheral Component Interconnect. A peripheral bus providing a high-speed data path between the CPU and the peripheral devices such as a monitor, disk drive, or network.

J. PDF: Portable Document Format. The file format used by the Acrobat document-exchange-system software from Adobe.

K. RF: Radio frequency.

L. ROM: Read-only memory.

M. TCP/IP: Transmission control protocol/Internet protocol.

N. UPS: Uninterruptible power supply.

O. USB: Universal serial bus.

P. WAN: Wide area network.

Q. WAV: The digital audio format used in Microsoft Windows.

R. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.

S. Windows: Operating system by Microsoft Corporation.

T. Workstation: A PC with software that is configured for specific, limited security-system functions.

1.04 ACTION SUBMITTALS

A. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a location on Drawings. Test and evaluation data presented in Product Data shall comply with SIA BIO-01.

B. Shop Drawings: Include plans, elevations, sections, details, and attachments to other work.

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 Parts 2 and 3.
3. Wiring Diagrams. For power, signal, and control wiring. Show typical wiring schematics including the following:

    a. Workstation outlets, jacks, and jack assemblies.
    b. Patch cords.
    c. Patch panels.

4. Cable Administration Drawings: As specified in "Identification" Article.
5. Battery and charger calculations for central station, workstations, and controllers.

C. Other Action Submittals:

1. Project planning documents as specified in Part 3.

1.05 INFORMATIONAL SUBMITTALS

A. Field quality-control reports.

1.06 CLOSEOUT SUBMITTALS

A. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals:

1. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM of the hard-copy submittal.

2. System installation and setup guides with data forms to plan and record options and setup decisions.

1.07 QUALITY ASSURANCE

A. Installer Qualifications: An employer of workers trained and approved by manufacturer.

1. Cable installer must have on staff a registered communication distribution designer certified by Building Industry Consulting Service International.

B. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

C. Comply with NFPA 70, "National Electrical Code."

1.08 DELIVERY, STORAGE, AND HANDLING

A. Server, Workstations, and Controllers:

1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 deg F, and not more than 80 percent relative humidity, noncondensing.
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 the same designations assigned to materials and equipment for recording in the system labeling schedules that are generated by software specified in "Cable and Asset Management Software" Article.
4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.09 PROJECT CONDITIONS

A. Environmental Conditions: System shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Control Station: Rated for continuous operation in ambient conditions of 60 to 85 deg F and a relative humidity of 20 to 80 percent, noncondensing.
2. Indoor, Controlled Environment: NEMA 250, Type 1 enclosure. System components, except the server, installed in temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of 36 to 122 deg F dry bulb and 20 to 90 percent relative humidity, noncondensing.
3. Indoor, Uncontrolled Environment: NEMA 250, Type 4 enclosures. System components installed in non-air-conditioned non-temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of 0 to 122 deg F dry bulb and 20 to 90 percent relative humidity, noncondensing.
4. Outdoor Environment: NEMA 250, NEMA 250, Type 4X enclosures. System components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of minus 30 to plus 122 deg F dry bulb and 20 to 90 percent relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 85 mph and snow cover up to 24 inches thick.
5. Hazardous Environment: System components located in areas where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers shall be rated, listed, and installed according to NFPA 70.

6. Corrosive Environment: For system components subjected to corrosive fumes, vapors, and wind-driven salt spray in coastal zones, provide NEMA 250, Type 6P enclosures.

PART 2 - PRODUCTS

2.01 MANUFACTURERS

A. Basis-of-Design Product: Subject to compliance with requirements, provide S2

2.02 CONTROLLERS

A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the server for controlling its operation.
B. Subject to compliance with requirements in this article, manufacturers may use multipurpose controllers.
C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924.
D. Alarm Annunciation Controller:

1. The controller shall automatically restore communication within 10 seconds after an interruption with the field device network, with dc line supervision on each of its alarm inputs.

a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions.

1) Support multiple supervised alarm inputs per door control unit with time zone disable feature, and programmable shunt delay timer.
2) Supervision of alarm points can be either two (alarm, reset) or four state (trigger, reset, open and short) determined at software configuration.
3) Provide a forced-door entry with ajar alarm. Forced-door alarm shall have a shunt delay timer. Ajar alarm shall have a programmable delay timer.
4) Support adding name of alarm in a field and additional information about each alarm in a “notes” field.
5) Support prioritizing of alarms to multiple levels.
6) Support linking specific alarms to relay control devices.
7) Include a graphical alarm editing application that shall allow user to define alarms including graphical maps. Animated icons shall be placed on maps to indicate standard alarm types such as fire and break-in. Four levels of zoom shall be provided for each alarm.
8) Require acknowledgment text so personnel monitoring alarms shall provide response information.
9) Include an alarm monitor application separate from main software which shall display alarms graphically in priority with which they were programmed. Application shall be able to be run from any workstation. Allow alarm acknowledgment from any workstation with synchronization between workstations.
10) Provide alarm monitor with capability to display a user portrait in response to valid or invalid access attempts.
11) Provide alarm monitor with support for standard sound cards and .wav files so user-defined sounds can be played for alarms.
12) Log off with password shall be required to quit alarm monitor.
13) Programmable requests for incident reports.
14) Support up to four floor maps per alarm input, available within one double click.

15) Directly on the alarm reported on the alarm monitor.

b. Alarm-Line Supervision:

1) Transmit alarm-line-supervision alarm to the central station during the next interrogation cycle after the abnormal current condition.

c. Outputs: Managed by server software. Provide multiple programmable and user-defined outputs, which are suitable for wiring as normally open or normally closed. Output relays shall be thermally or fused protected.

1) Multiple Form C contacts, rated 30 V dc maximum at 2 A.
2) Supervisory Function: Relay 0 on first board installed. Opens on system fault.
3) Tamper Alarm: Onboard switch.
4) Polarity selectable on all relays; via software or jumper.

E. Entry-Control Controller:

1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, biometric personnel identity-verification devices, door strikes, magnetic latches, gate and door operators, and exit push buttons.

a. Operate in a fully distributed manor maintaining all card holder records privileges, alarm programming, holidays, etc., downloaded from the server.
b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:

1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
2) Privileges shall include, but are not limited to, time of day control, day of week control, group control, and visitor escort control.

c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:

a. Multiple auxiliary inputs, refer to the alarm annunciation controller paragraph in this Article for requirements.

3. Outputs:

a. Multiple auxiliary outputs, refer to the alarm annunciation controller paragraph in this Article for requirements.

4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.

5. Communication Problems: For periods of loss of communication with the server, the controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.

    a. Store a minimum of 1000 transactions during periods of communication loss between the controller and access-control devices for subsequent upload to the server on restoration of communication.

6. Controller Power: UL listed power supply filtered and regulated output; built-in battery charging circuit; self-resetting output fuse; steel hinged locking cover enclosure with conduit knockouts; modular for optional fire alarm control and individual fused zone outputs. Include an anti-tamper switch to signal opening.

    a. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
    b. Backup Power-Supply Capacity: 90 minutes of battery supply. Submit battery and charger calculations.

2.03 CARD READERS, CREDENTIAL CARDS, AND KEYPADS

A. Basis-of-Design Product: Subject to compliance with requirements, provide HID iClass RMK40 Keypad Card Readers.

2.04 PUSH-BUTTON SWITCHES

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. Dynalock Corporation.
2. Securitron.
3. SDC.

B. Delay on Relock Palm Switch: NFPA 101.

1. Red pushbutton.
2. Switch non-electronic, pneumatic delay, 30-second minimum, SPDT-DB (Form Z) rated 10A at 125 Vac.
3. Single gang faceplate, US32D stainless steel, silkscreened "PUSH TO EXIT" in red.

2.05 DOOR SWITCHES

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. GE Security.
2. Honeywell.
3. GRE.
4. Optex.
5. Amseco.

B. Description: Single pole double throw Balanced-magnetic switch, complying with UL 634, installed on frame with integral overcurrent device to limit current to 80 percent of switch

capacity. Bias magnet and minimum of two encapsulated reed switches shall resist compromise from introduction of foreign magnetic fields.

C. Flush-Mounted Switches: Unobtrusive and flush with surface of door and window frame.

D. Overhead Door Switch: Balanced-magnetic type, listed for outdoor locations, and having door-mounted magnet and floor-mounted switch unit.

E. Remote Test: Simulate movement of actuating magnet from master control unit.

2.06 DOOR HARDWARE INTERFACE

A. Electric Door Locking Hardware: Use end-of-line resistors to provide power-line supervision. Signal switches shall transmit data to controller to indicate when the hardware is not engaged and the hardware is unlocked, and they shall report a forced entry. Power and signal shall be from the controller. Electric Door Locking Hardware is specified in Section 087100 "Door Hardware."

2.07 IP VIDEO INTERCOM

A. Basis-of-Design Product: Subject to compliance with requirements, provide Aiphone or approved equivalent.

B. Door Stations, "IC" as indicated on drawings:

1. Fixed Door Station: Model IX-DV series.

a. Faceplate: Die-cast zinc.
b. Exact mounting type and location, coordinate with architect.
c. SIP Compatible
d. Microphone
e. Speaker
f. Fixed camera
g. Call button
h. Vandal resistant
i. Weather resistant
j. Operating Temperature: 14 deg. F to 140 deg. F (minus 10 deg. C to 40 deg. C).
k. Provide CAT 6 cable and connectivity.
l. Provide and coordinate with manufacturers system and mounting requirements.

C. Master Stations, "MIC" as indicated on drawings:

1. Master Station: Model IX-MV series.

a. An IP addressable video master station with a 7-inch color LCD monitor and SIP compatible.
b. It can be wall- or desk-mounted (desk stand included).
c. The IX-MV series offers handset (duplex) and hands-free (VOX/PTT) communication and call up to 500 other IX stations. It connects directly to a network using CAT 6 cable. This station requires an 802.3af compliant Power-over-Ethernet network.
d. Provide CAT 6 cable and connectivity.

e. Power: PoE switch by others.
f. Provide and coordinate with manufacturers system and mounting requirements.

D. Mobile Sub Master Stations:

1. IP Relay Adaptor: Model IXW-MA series.

a. One unit per 8 mobile apps in the system.
b. Power: PoE switch by others.
c. Provide and coordinate with manufacturers system and mounting requirements.

2. Mobile App Sub Master Station: Model IX-Mobile App.

a. Mobile App Sub Master Station for Smartphones and Tablets.
b. Provides station functionality to answer calls and unlock doors.
c. 4 speed-dial buttons can be programmed to call, page, or monitor.
d. Provide and coordinate with manufacturer's system requirements.
e. Coordinate with owner for available App on owner mobile device within App download. Provide support for system functions and door operations.

2.08 CABLES

A. General Cable Requirements: Comply with requirements in Section 280513 "Conductors and Cables for Electronic Safety and Security" and as recommended by system manufacturer for integration requirement.

PART 3 - EXECUTION

3.01 EXAMINATION

A. 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.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.02 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with ANSI/TIA/EIA 606-A, "Administration Standard for Commercial Telecommunications Infrastructure."

C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom 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 controller features and access requirements.
3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
4. Set up groups, facility codes, linking, and list inputs and outputs for each controller.
5. Assign action message names and compose messages.
6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
7. Prepare and install alarm graphic maps.
8. Develop user-defined fields.
9. Develop screen layout formats.
10. Propose setups for guard tours and key control.
11. Discuss badge layout options; design badges.
12. Complete system diagnostics and operation verification.
13. Prepare a specific plan for system testing, startup, and demonstration.
14. Develop acceptance test concept and, on approval, develop specifics of the test.
15. Develop cable and asset-management system details; input data from construction documents. Include system schematics and Visio Technical Drawings in electronic format.

D. 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.

3.03 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Construction."

B. Install cables and wiring according to requirements in Section 280513 "Conductors and Cables for Electronic Safety and Security."

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental airspaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

D. Install LAN cables using techniques, practices, and methods that are consistent with Category 5E rating of components and fiber-optic rating of components, and that ensure Category 6 and fiber-optic performance of completed and linked signal paths, end to end.

E. 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. Boxes above ceiling level in occupied areas of the building shall not be considered accessible. 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.

F. Install end-of-line resistors at the field device location and not at the controller or panel location.

3.04 CABLE APPLICATION

A. Comply with TIA 569-B, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

C. TIA 485-A Cabling: Install at a maximum distance of 4000 ft.

D. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from controller to the reader is 250 ft., and install No. 20 AWG wire if maximum distance is 500 ft..
3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the controller.
4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

E. Install minimum No. 16 AWG cable from controller to electrically powered locks. Do not exceed 500 ft..

F. Install minimum No. 18 AWG ac power wire from transformer to controller, with a maximum distance of 25 ft..

3.05 GROUNDING

A. Comply with Section 280526 "Grounding and Bonding for Electronic Safety and Security."

B. Comply with IEEE 1100, "Recommended Practice for Power and Grounding Electronic Equipment."

C. 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.

D. Bond shields and drain conductors to ground at only one point in each circuit.

3.06 INSTALLATION

A. Install cabling, card readers, **video intercom,** electronics safety and associated electronic safety & security hardware.

B. Integrate Access Control system with the campus wide Access Control system.

3.07 IDENTIFICATION

A. In addition to requirements in this article, comply with applicable requirements in Section 260553 "Identification for Electrical Systems" and with TIA/EIA 606-A.

B. Label each device in each cabinet, rack, or panel.

3.08 SYSTEM SOFTWARE AND HARDWARE

A. Develop, install, and test software and hardware, and perform database tests for the complete and proper operation of systems involved. Assign software license to Owner.

3.09 FIELD QUALITY CONTROL

A. Devices and circuits will be considered defective if they do not pass tests and inspections.

B. Prepare test and inspection reports.

3.10 DEMONSTRATION

A. Train Owner's maintenance personnel to adjust, operate, and maintain security access system. See Section 017900 "Demonstration and Training."

END OF SECTION
09/25/2019-Addendum 3