|  |
| --- |
| **Revision History** |
| **Revision Date** | **Section / Nature of Revision** |
| **03/01/2017** | Document Issued |
| **10/20/2021** | 2.3 B: changed run time during outage from 30 minutes to 1 hour.2.3 I: updated single door Controller part number.2.4 F: updated reader part number.2.5 A: deleted verbiage and updated electric strike part number.2.5: added B and C section.3.2: added E through G section.3.5 A Deleted last sentence relating to control diagram.3.6 E: deleted section E (end of line resistors).3.12 B: deleted 3.12 B.3) through 5).3.14 F: changed verbiage. |
| **11/18/2021** | 2.5 C: changed Locknetics to DynaLock.3.2 G: changed Locknetics to DynaLock. |
| **6/5/2024** | 2.5 C: changed DynaLock 3101 to DynaLock 3101ES.3.2 G: changed DynaLock 3101 to DynaLock 3101ES. |
| **8/29/24** | 1.8 D: added that all submittals must be approved by the Engineer of record and the Owner.3.2 E 2 and 3: added single panel shall be powered by TRG2440… and Panels 2 through 4 shall be powered by ALTV244…3.2 F 1, 5, 6a 7: F: removed with strikes; 1: removed 2PX2, added panel and removed six; 5: removed parallel and added series; 6: removed AL1012UXB and added AL1024ULXB2, a: added if remotely powered use AL1024ULXPD16; and 7: removed strike and added electric locking device. |

**PART 1 GENERAL**

1.1 RELATED DOCUMENTS

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

1.2 SUMMARY

A. Provide a TCP/IP Access Control System. The intent is for this Contractor to provide the devices, connections, testing, programming, documentation, etc. for a working system (including any missing or defective cabling).

B. The security access system shall have the following:

1. Regulate access through specific doors.
2. Credential cards and readers.
3. Monitoring of field-installed devices.
4. Reporting.

1.3 RELATED SECTIONS

1. Section 08 71 00 Door Hardware
2. Section 26 05 19 Building Wire and Cable
3. Section 26 05 33.16 Boxes
4. Section 26 05 53 Electrical Identification
5. Section 27 10 00 Structured Cabling
6. Section 28 30 00 Intrusion Detection System

1.4 DEFINITIONS

1. Central Station: A PC with software designated as the main controlling PC of the security access system. Where this term is presented with initial capital letters, this definition applies.

B. ACU: Access Control Unit

C. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.

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

E. GFI: Ground fault interrupter.

F. 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.

G. I/O: Input/Output.

H. LAN: Local area network.

I. WAN: Wide area network.

J. LED: Light-emitting diode.

K. RF: Radio frequency.

L. ROM: Read-only memory. ROM data are maintained through losses of power.

M. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

N. UPS: Uninterruptible power supply.

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

1.5 SYSTEM DESCRIPTION

A. Intent is for the Access Control System to be IP based. Existing system software: Paxton, Net2.

1) Multi-user multi-tasking to allow for independent activities and for monitoring to occur simultaneously at different workstations.

2) Graphical user interface to show pull-down menus and a menu tree format.

3) Password-protected operator login and access.

B. Network, connecting the system, shall be via a dedicated VLAN on Owner’s network.

1.6 QUALIFICATION AND QUALITY ASSURANCE

A. Manufacturer: manufacturer's authorized representative, trained and approved for installation of units required for this Project, with at least five years documented experience. Installing and servicing office to be located within a 50-mile radius of Pinellas County. Pinellas County Schools approved vendors only! See Pinellas County Schools representative for vendor to be used.

B. Installer: company specializing in access control systems with five years’ experience, certified by Florida State Licensing Board as an access control system installing contractor and maintain installation, service and technical staff within 50 miles of Pinellas County. The Contractor shall provide evidence of qualifications upon request. Pinellas County Schools approved vendors only! See Pinellas County Schools representative for vendor to be used.

C. Installer shall employ workers trained and approved by manufacturer. The cable installer shall have on staff a registered communication distribution designer certified by Building Industry Consulting Service International.

D. The Contractor shall be prepared to offer a service contract for the maintenance of the system after the warranty period.

E. Certifications:

1. Paxton Integrator (demonstrates competency and experience in the Paxton software and hardware) Paxton Net 2 Essential and Net 2 Advanced Certificates required.
2. Paxton Certified Staff - minimum of three within 50 miles of Pinellas County. Paxton Net 2 Essential and Net 2 Advanced Certificates required.

F. Electrical components, devices and accessories: listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to the Authority Having Jurisdiction (AHJ) and marked for intended use.

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

H. Comply with SIA DC-03 and SIA DC-07.

1.7 PERFORMANCE REQUIREMENTS

A. Existing security access system has a single database for access-control and credential-creation functions.

B. Distributed processing: system shall be a fully distributed processing system so that information including time, date, valid codes, access levels and similar data is downloaded to Controllers so that each Controller makes access-control decisions for that location. Intermediate Controllers for access control shall not be used. If communications to Central Station are lost, all Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the Central Station.

C. System network requirements:

1. Interconnect system components and provide automatic communication of status changes, commands, field-initiated interrupts and other communications required for proper system operation.
2. Communication shall not require operator initiation or response and shall return to normal after partial or total network interruption such as power loss or transient upset.
3. The system shall automatically annunciate communication failures to the operator and identify the communication link that has experienced a partial or total failure.

D. Existing Central Station shall provide operator interface, interaction, display, control and dynamic and real-time monitoring. The existing Central Station shall control system networks to interconnect all system components, including workstations and field-installed Controllers.

E. Field equipment shall include Controllers, sensors and controls. The Controllers shall serve as an interface between the Central Station and sensors and controls. Data exchange between the Central Station and the Controllers shall include down-line transmission of commands, software and databases to Controllers. The up-line data exchange from the Controller to the Central Station shall include status data such as alarms, status reports and entry-control records. The Controllers are classified as alarm-annunciation or entry-control type.

F. System response to alarms: alarms shall be annunciated at the Central Station within one second of the alarm occurring at a Controller or device controlled by a local Controller and within 100 milliseconds if the alarm occurs at the Central Station. Alarm and status changes shall be displayed within 100 milliseconds after receipt of data by the Central Station. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within five seconds of alarm receipt at the security console.

G. False alarm reduction: the design of Central Station and Controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

H. Error detection: a cyclic code error detection method shall be used between Controllers and the Central Station, which shall detect single- and double-bit errors, burst errors of eight bits or less and at least 99 percent of all other multi-bit and burst error conditions. Interactive or product error detection codes alone will not be acceptable. A message shall be in error if one bit is received incorrectly. The system shall retransmit messages with detected errors. A two-digit decimal number shall be operator assignable to each communication link representing the number of retransmission attempts. When the number of consecutive retransmission attempts equals the assigned quantity, the Central Station shall print a communication failure alarm message. The system shall monitor the frequency of data transmission failure for display and logging.

I. Data line supervision: The system shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

J. Door hardware interface: coordinate with Division 08 Section that specifies door hardware required to be monitored or controlled by the security access system. The Controllers in this section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 08 Section to function with the controls and PC-based software and hardware in this section.

1.8 SUBMITTALS (submit three copies of the requested data)

A. Shop drawings:

1) Product Data: For each type of product indicated (include dual reed door contacts and local alarm device when door is propped open). Include operating characteristics, 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.

2) Location and elevations of equipment to be mounted.

3) Door rough-In (indicated door hardware): for each door, provide a raceway rough-in drawing detailing the means and methods to provide access control and power cabling. This includes cabling within door frame and door.

3) Battery calculations for Controllers and door locks.

4) Copy of contractor license and RCDD certificate.

B. Project planning documents as specified in Part 3.

C. Operation and maintenance data:

1. Manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware and PDF files on CD-ROM or USB drive of the hard-copy submittal.
2. System installation and setup guides, with data forms to plan and record options and setup decisions.
3. The Engineer of record and the Owner must approve all submittal packages.

1.9 DELIVERY, STORAGE and HANDLING

A. Controllers:

1. Store in temperature and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50- and 85-degree F and not more than 80% 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 designations that have been assigned to materials and equipment for recording in the system labeling schedules that are generated by cable and asset management system specified in Part 2.
4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.10 PROJECT CONDITIONS

A. Preconstruction inspection and deficiency list: this Contractor shall inspect doors prior to starting construction. Any deficiencies that would affect the access control system installation shall be brought to the Owner’s attention. It would be the Owner’s decision whether to correct these items independent of this Contractor or to add the scope of work to this Contract.

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

1. Interior, controlled environment: the system components, except Central Station control unit, installed in temperature-controlled interior environments shall be rated for continuous operation in ambient conditions of 36-to-122-degree F dry bulb and 20 to 90 percent relative humidity, noncondensing. NEMA 250, Type 1 enclosure.
2. Exterior environment: the system components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of minus 30 to plus 122-degree 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. NEMA 250, Type 3R enclosures.

**PART 2 PRODUCTS**

2.1 APPLICATION SOFTWARE – SECURITY ACCESS SYSTEM

A. Paxton Access, IP Access Control System Headend PC/Software (Net2), Enrollment Center and Access Cards are existing.

B. Controller Software:

1. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about access control, alarm monitoring, linking functions and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints and the latest value or status of points connected to that Controller, shall be maintained in the Controller.
2. The following functions shall be fully implemented and operational within each Controller:
3. Monitoring inputs.
4. Controlling outputs.
5. Automatically reporting alarms to the Central Station.
6. Reporting of sensor and output status to Central Station on request.
7. Maintaining real time, automatically updated by the Central Station at least once a day.
8. Communicating with the Central Station.
9. Executing Controller resident programs.
10. Diagnosing.
11. Downloading and uploading data to and from the Central Station.
12. Controller operations at a location:
13. Connect to communications loop via category cable and the Owner’s LAN/WAN equipment. Globally operating I/O linking and anti-passback functions between Controllers within the same location without Central Station or workstation intervention. Linking and anti-passback shall remain fully functional within the same location even when the Central Station or workstations are offline.
14. In the event of communications failure between the Central Station and a location, there shall be no degradation in operations at the Controllers at that location.
15. Buffered events shall be handled in a first-in-first-out mode of operation.
16. Individual Controller operation:
17. Controllers shall transmit alarms, status changes and other data to the Central Station when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station. Buffer capacity for the latest 99,999 transactions shall be provided at each Controller.
18. Card-reader ports of a Controller shall be custom configurable for different card-reader formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.
19. Controllers shall provide a response to card-readers or keypad entries in less than 0.25 seconds, regardless of system size.
20. Controllers that are reset, or powered up from a non-powered state, shall automatically request a parameter download and reboot to its proper working state. This shall happen without any operator intervention.
21. Initial startup: when Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.
22. Failure mode: on failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.
23. Startup after power failure: after power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.
24. Startup after Controller failure: on failure, if the database and application software are no longer resident, Controllers shall not restart but shall remain in the failure mode until repaired. If database and application programs are resident, Controllers shall immediately resume operation. If not, the software shall be restored automatically from the Central Station.

C. Controller-to-Controller Communications:

1. Controller-to-Controller communications: via Owner’s LAN/WAN. The Contractor is to establish communication with input from Owner for port allocation.

D. Database Downloads:

1. All data transmissions from PC to a location and between Controllers at a location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a Controller is reset for any reason, it shall automatically request and receive a database download from the PC. The download shall restore data stored at the Controller to their normal working state and shall take place with no operator intervention.

2.2 SURGE AND TAMPER PROTECTION

A. Surge protection: protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor entry connection to components.

1. Minimum protection for power connections 120 Volts and more: auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."
2. Minimum protection for communication, signal, control and Low-Voltage power connections: comply with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits" as recommended by manufacturer for type of line being protected.

B. Tamper protection: tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control Station control-unit alarm display shall identify tamper alarms and indicate locations.

2.3 TCP/IP CONTROLLER

A. Provide intelligent, TCP/IP peripheral control unit, complying with UL 294, which stores time, date, valid codes, access levels and similar data downloaded from the Central Station or workstation for controlling its operation.

B. Controller battery backup: sealed lead acid, sized to provide run time during a power outage of 1 hour with a minimum of 7Ah capacity, complying with UL 924. Contractor to ensure Owner’s network switch (connected to access control system) shall be on an Owner provided UPS that is connected to an emergency power circuit within the closet.

C. Provide power supply for Controller/panel. Locate control in closets. Provide plug-in transformer for closets with single panels. Provide power supply for closets with multiple panels (acceptable manufacturer: Altronix ALTV244 or sized as required by number of panels).

D. 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.

1. Inputs: monitor dry contacts for changes of state that reflect alarm conditions. Provide at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.

E. Provide local entry control functions including communications with access-control devices such as card readers, door strikes and door operators.

1. Operate as a stand-alone portal with the Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.
2. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:
3. On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
4. Privileges shall include, but not be limited to, time of day control, day of week control, group control and visitor escort control.
5. 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.

F. Inputs:

1. Data from entry control devices.
2. Database downloads and updates from the Central Station that include enrollment and privilege information.

G. Outputs:

1. Indicate success or failure of attempts to use entry control devices and make comparisons of presented information with stored identification information.
2. Grant or deny entry by sending control signals to portal-control devices.
3. Maintain a date, time and location stamped record of each transaction and transmit transaction records to the Central Station.
4. Door prop alarm: if a portal is held open for longer than 20 seconds (adjustable), alarm shall sound. Provide recessed dual reed (position/status) door contacts with alarm hardware and associated cabling in jamb, opposite hinge location separate from the Intrusion System contact.
5. Power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
6. Data line problems: for periods of loss of communications with Central Station or when data transmission is degraded and generating continuous checksum errors, the Controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges and controlling portal control devices.

H. Intent is to use Owner’s LAN switches. the Installer shall notify Owner as to the number of ports required and coordinate as to which ports are to be utilized prior to connection.

I. Acceptable manufacturer: Paxton Access Net2 Plus, Single Door Controller (682-610-US). Reference drawings for locations and quantities of access doors and closets. Any equipment deviations or configuration modifications shall be pre-approved prior to bid.

2.4 MULTI-TECHNOLOGY, ENCODED PROXIMITY CARD READER

A. Encoded proximity card reader shall be Weigand output with passive detection that shall use a swept frequency, RF field generator to read the resonant frequencies of tuned circuits laminated into compatible credential cards. The resonant frequencies read shall constitute a unique identification code number.

B. Card reader shall respond to passage requests by generating a signal that is sent to the Controller.

C. Card reader shall be powered from its associated Controller, including its standby power source.

D. Mounting types shall be suitable for outdoors installation.

E. Provide with LED visual indicator (i.e., red, green, amber) and audio feedback representing status and activity information, easily discernible for the audibly or visually impaired.

F. Acceptable manufacturer: HID Plus Mini Mullion Reader, Model No. 6005BGB00. Substitutions must be pre-approved by Owner representative.

2.5 DOOR HARDWARE INTERFACE (Refer to Architect’s Door Hardware)

A. Electric door strikes: power and signal shall be from the Controller. Electric strike kit, power supply, etc. The electric strike kit shall be HES 9400 or 8000 series locks unless otherwise stated by the district representative. Refer to “Division 08, Access Door Hardware" to verify function of electric strike with door hardware.

B. Acceptable manufacturer for latch retraction: SDC LR100VDK. Substitutions must be pre-approved by Owner representative.

C. Delayed Egress

1. In addition to the DynaLock 3101ES and power supply described in 3.2 G, the following devices are required. The Von Duprin 050271-00 exit switch is the only acceptable request to exit switch. The Securitron PZ1 is preferred for an interior annunciator and ADI OE-1GANGDRSR for the exterior annunciator. The magnetic locks are different for the interior and the exterior. The preferred interior magnet is the SDC part No. 1581 and for the exterior the Schlage part No. SFX 7410. Any substitutions must be pre-approved by the Owner representative.

2.6 CABLES

A. The Contractor shall provide cabling per manufacturer’s recommendations for a working system. All access control system cabling shall be plenum rated and consistent with Owner’s standards. All network cabling shall match Division 27 10 00 Structured Cabling specifications or pre-approved equal.

**Part 3 EXECUTION**

3.1 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 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.

3.2 Installation of Access Control System

A. Install access control system as indicated, in accordance with equipment manufacturer's written instructions.

B. The Contractor shall provide all equipment required for the installation of the access control system. To include electric strikes.

C. Contractor shall install all equipment, conduit, wire, terminal strips and related equipment. All wiring shall be closed to verify continuity. The main control panels shall be installed in either an IDF or MDF room and have an electrical system grounding connection and LAN/WAN connection.

D. Provide concealed conduit from door jambs to above finished ceilings. Wiring to terminal cabinets and other device locations shall be run without conduit in ceiling spaces. All wiring shall be in accordance with N.E.C.

E. One to four Net2 Controllers at one location:

1. Use a single 12V 7Ah battery in each panel.
2. A single panel shall be powered by a TRG2440 transformer or equivalent.
3. Panels 2 through 4 shall be powered by an ALTV244 power supply.

 F. Five to nine Net2 Controllers at one location:

1. Mount Altronix Trove panel on wall using all mounting points.
2. If on drywall use a minimum of 3/16” toggle bolts.
3. If on masonry wall use a minimum of 3/16” masonry screw.
4. If on wood use a minimum of No. 8 screws.
5. Battery backup will be two 12V 18Ah NB No. 2 batteries in series.
6. The power supply will be Altronix AL1024ULXB2.
7. If remotely powered use AL1024ULXD16.
8. The power distribution will be Altronix PD16W.
9. The Controller and associated locking device will be wired to the same single fuse.

 G. Delayed egress configurations:

1. Use Net2 panel and DynaLock 3101 wired as 24VDC.
2. The power supply shall be Altronix AL600ULX and capable of powering two Net2 panels and two electric strike 3101 panels.

3.3 FIRESTOPPING

A. All penetrations of rated walls, floors, or ceilings shall be through a metallic conduit sleeve fire stopped with a UL listed firestopping product. See project drawings for penetration details.

B. Penetrations of non-rated masonry walls shall have a conduit sleeve.

3.4 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."

C. Obtain detailed Project planning forms from manufacturer of access-control system and develop custom forms to suit the Project. Fill in all data available from the Project plans, specifications and publish as Project planning documents for review and approval.

1. For each location, record setup of Controller features and access requirements.
2. Propose start and stop times for time zones and holidays and match up access levels for doors.
3. Set up groups, facility codes, linking and list inputs and outputs for each Controller.
4. Assign action message names and compose messages.
5. Set up alarms. Establish interlocks between alarms and intruder detection.
6. Complete system diagnostics and operation verification.
7. Prepare a specific plan for system testing, startup and demonstration.
8. Develop acceptance test concept and, on approval, develop specifics of the test.

3.5 COMPLETION AND TESTING

A. Furnish to the Owner a written report which certifies that all initiating devices have been tested and which indicate the result of the inspection. Additionally, furnish to the Owner, three sets of operation and maintenance manuals with parts list and other information necessary for the proper operation and maintenance on the system, as installed. Include three copies of complete troubleshooting and repair manuals. Provide Owner with a CD-ROM copy (AutoCAD 2014 or later) and two printed copies as-built drawings indicating location of conduit, junction boxes and zoning of each individual device.

B. Upon completion of installation, the system shall be completely checked out and tested by a factory-authorized representative, to determine that the system was tested and installed in accordance with the manufacturer's instructions and all applicable codes. Results of the check out and testing shall be reported in writing to the Architect/Engineer. The written report shall precede or accompany the Contractor's request for acceptance inspection for work under this Section. This representative shall prepare an inspection report for the Owner and instruct the Owner's personnel in the operation of the system.

C. Provide eight effort hours of onsite training for two people on the operation, maintenance, troubleshooting and repair of the system at the Contractor's expense. Training shall be certified by the manufacturer and be at different times for each person. Transportation, room and board, where needed, shall be the responsibility of the trainer. Furnish Engineer with a list of attendees.

D. The Contractor, at no cost to the Owner, shall immediately replace all equipment, devices and/or work found to be defective.

E. Before testing the access control system transmission from the project site to the central control station, coordinate with the Owner’s Project representative. Personnel shall be available to verify a successful and trouble-free transmission signal.

F. Site Test:

1. Check and test installation for shorts, ground and circuit continuity.
2. Cables: test free from opens, grounds, or crosses (shorts) between conductors.
3. Walk-test system for proper function and operation. Ensure proper zoning of devices.
4. Test all functions on access control panels for proper functions and operations.
5. Verify signals are properly received by the district.
6. Check for proper standby battery backup in access control panels and remote power supplies.
7. Verify remote power supplies are UL listed.
8. Inspect and test cabinet tampers on access control cabinets.
9. Verify raceway cover is properly color-coded.

3.6 CABLING

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

B. Wiring method: install wiring in raceway and cable tray. Use NRTL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway and wiring except in unfinished spaces.

C. Install cables without damaging conductors, shield, or jacket.

D. 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 to be 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.

3.7 CABLE APPLICATION

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

B. Do not exceed cabling recommended lengths.

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

D. Card Readers:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. For greater distances, install "extender" or "repeater" modules recommended by the manufacturer of the Controller.
3. Install minimum No. 18 AWG shielded cable to readers that draw 50 mA or more.

3.8 GROUNDING

A. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."

B. Comply with IEEE 1100, "Power and Grounding Sensitive 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. Signal Ground:

1. Terminal: locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
2. Bus: mount on wall of main equipment room with standoff insulators.
3. Backbone cable: extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.9 IDENTIFICATION

A. In addition to requirements in this Article, comply with applicable requirements in Division 26 Section "Identification for Electrical Systems" and with TIA/EIA-606.

B. Using cable and asset management software specified in Part 2, develop cable administration drawings for system identification, testing and management. Use unique, alphanumeric designation for each cable and label cable and jacks, connectors and terminals to which it connects with same designation. Use logical and systematic designations for facility's architectural arrangement.

C. 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 particular device as shown.
2. Each wire connected to building mounted devices is not required to be numbered at the device if the color of the wire is consistent with the associated wire connected and numbered within the panel or cabinet.

D. At completion, cable and asset management software shall reflect as-built conditions.

3.10 FIELD QUALTIY CONTROL

A. Manufacturer's field service: engage a factory-authorized service representative to inspect, test and adjust field-assembled components and equipment installation, including connections and to assist in field testing. Report results in writing.

B. Remove and replace malfunctioning devices and circuits and retest as specified above.

3.11 PROTECTION

A. Maintain strict security during the installation of equipment and software.

3.12 DEMONSTRATION

A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate and maintain security access system.

B. 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.

3.13 PROJECT RECORD DRAWINGS

A. Submit documents under the provisions of Division 1.

B. Include location of end-of-line devices.

3.14 WARRANTY

A. Submit data under provisions of Division 1.

B. Include letter from authorized manufacturer representative (addressed to the district) stating that the system is operational and in compliance with warranty requirements. Include five copies of full manufacturer’s published warranty for parts and components to be provided.

C. Provide warranty response information inside alarm system control panel.

D. Warranty shall allow the district to repair vandalized areas without voiding the total system warranty.

E. The system shall be warranted with the electric components covered for a period of one-year full maintenance (parts, wiring and labor) provided by Contractor or manufacturer’s authorized representative. The remaining elements including wiring and zone controls shall be warranted for a period of two years from the date of acceptance by the Owner against defective materials, design, workmanship and improper adjustment. Any defective materials shall be replaced at no expense (parts or labor) to the Owner providing they do not show abuse. The representative must be able to respond to warranty calls within 12 hours of notice, whether oral or written.

F. This Contractor shall assist in and install software updates on the Owner’s system throughout the warranty period (software and labor to install are to be included within this bid), if needed.

\*\*\***END OF SECTION\*\*\***