Electronics Services Access Control Standards

PART 1 – GENERAL

1.1 SUMMARY

A. The minimum criteria for the design, supply, installation, and activation of the Security Management System, which shall be a modular and networkable access control system. The system shall be compatible with existing University of Delaware Campus Wide Security Management System. Equipment provided shall be connected to University of Delaware Host Computer. System shall include all engineering and system design equipment, software, programming and data input, system checkout installation and acceptance testing.

1.2 GENERAL

A. Section includes:
   1. Operating system and applicable software.
   2. Design and input of system database.
   3. Control panel systems.
   4. Card readers and cards.

B. Related sections:
   1. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 1 Specification Sections, apply to this Section.
   2. Division 8: Door Hardware.

C. Acceptable contractors:
   1. MSA Systems Integration
   2. TYCO

1.3 REFERENCES

A. Federal Communications Commission (FCC):
   1. FCC Part 15: Radio Frequency Devices.
   2. FCC Part 68: Connection of Terminal Equipment to the Telephone Network.

B. Underwriters Laboratories (UL):
   1. UL 294: Access Control System Units.
   2. UL1076: Proprietary Burglar Alarm Units and Systems.

C. National Fire Protection Association (NFPA):
   1. NFPA 70: National Electrical Code.

D. Electronic Industries Alliance (EIA):
   1. RS-232C: Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange.
   2. RS-485: Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems.
   3. EIA/TIA 606.

E. International Building Code.

F. Security Industry Association:
   1. SIA CP-01
   2. SIA CP-07

1.4 DEFINITIONS

A. No substitutes: The exact make and model number identified in this specification shall be provided without exception.

B. Or equal: Any item may be substituted for the specified item provided that in every technical sense, the substituted item provides the same or better capability and functionality.

C. Or approved equal: Owner may offer a substitute for the specified item for approval. The proposed substitution must, in very technical sense, provide the same or better capability and functionally as the specified item. Such requests for approval shall be submitted in accordance with the provisions of Article 1.06 SUBMITTALS, prior approvals, and must be obtained within the time frames outlined.

D. Company: Used to describe an access control group (cardholders and privileges).

1.5 SYSTEM DESCRIPTION

A. The Security Management System shall integrate Access Control, Alarm Monitoring, and Database Management. Provide modular and networkable system architecture. The system shall include the following capabilities:

   1. Direct wire operation, local area network (LAN) (Ethernet), or wide area network (WAN) operation or remote operation via network.
   2. Distributed architecture shall allow controllers to operate independently of the host. The architecture shall place key access decisions, event/action processing, and alarm monitoring functions within the controllers, eliminating degraded mode operation.
   3. Communication between the server/workstations, controllers, and other hardware shall be via Pro-Watch NT software and shall be compatible with existing University Security Management System.

4. Compatible with existing University Security Management System. Proprietary software programs and control logic information used to coordinate and drive system hardware shall be stored in programmable read-only memory (PROM).
5. Upgrades to the hardware and software shall occur seamlessly without the loss of database, configurations, or historical report data.
6. Firmware updates and revisions shall be downloaded to the system via network or system communication.
7. Both supervised and non-supervised alarm point monitoring shall be provided.
8. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.
9. Manual or automatic arming or disarming alarm points shall be performed by time of day and day of week.
10. Database partitioning shall provide the option to restrict access to sensitive information by user ID.
11. Door Hardware Interface: Coordinate with Division 8 Sections that specify 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 8 Sections to function with the controls and PC-based software and hardware in this Section.

B. Security Management System Door/Elevator Operation:
   1. Residential Halls card reader doors and monitored doors to use SDM 100. SDM to be mounted in a secure enclosure; Hammond 1439R4 with a lock to accept a Best Locks core. In cases where 2 doors are wired to one SDM 100, one door to use MSS200-7 door contact and other door to use PFC48Y door contact.
   2. Valid Card Read shunts door position alarm and activates electric door operator or unlocks door hardware for entry.
   3. Doors forced open shall initiate immediate alarm signal.
   4. Doors providing access to stairs propped open after valid card read or valid request to exit for more than 15 seconds shall cause a local alarm horn audible alert at door location and initiate an alarm signal.
   5. Loss of power to that part of the access control system which locks the doors shall automatically unlock the doors.
   6. The doors shall be arranged to unlock from a manual push button Request to Exit, unlocking device located 40 inches to 48 inches vertically above the floor and within 5 feet of the secured doors. Ready access shall be provided to the manual unlocking device and the device shall be clearly identified by a sign. When operated, the manual unlocking device shall result in direct interruption of power to the lock – independent of the access control system electronics – and the doors shall remain unlocked for a minimum of 30 seconds.
   7. Activation of the building fire alarm system, shall automatically unlock the doors, and the doors shall remain unlocked until the fire alarm system has been reset.

1.6 SUBMITTALS

A. General: Comply with Division 01 and Section 26 0101.

B. Shop drawings and schematics: These shall depict the system in final "as-built" configuration. The following items shall be provided:
   1. Connection diagrams for all interfacing equipment.
   2. List of connected equipment, including model numbers.
   3. Locations for all major equipment components installed under this specification.
   4. Field wiring diagrams and panel wire lists.
   5. Software and data entry forms.

C. Product data:

   The following shall be provided:
   1. Technical data sheets.
   2. A complete set of user guides, installation manuals, and operation manuals.

D. Quality assurance submittals: The following shall be provided:

   1. Checkout report: The Contractor shall provide the owner with a checkout report for each piece of equipment. The report shall include:

      - Complete list of each device.
      - The date it was tested and by whom.
      - The date it was re-tested indication that every device was tested successfully.
      - Final test report indicating that very device was tested successfully.

   2. Manufacturer's instructions: The Contractor shall deliver a set of System Operation and Maintenance manuals to the Owner.
   3. Notice of completion: When the final acceptance has been satisfactory completed, the Owner shall issue a notice of completion to the Contractor.
   4. Copies on DVD of System Software, Data Files (two copies).
   5. As-built, CAD generated drawings (four copies) plus electronic files compatible with AutoCAD (two copies).

1.7 QUALITY ASSURANCE

A. Systems shall be listed and meet the requirements of UL 294 and UL 1076 and be listed for intended purpose.

1.8 DELIVERY, STORAGE, AND HANDLING

A. General: Delivery, storage, and handling of the system components shall be in accordance with the Division 1 Product Requirements Sections.

B. Ordering: The manufacturer's ordering instructions and lead-time requirements shall be followed in order to avoid construction delays.

C. Delivery: The system components shall be delivered new, current manufacturer's production and be delivered in the manufacturer's original, unopened, and undamaged containers with the intact identification labels.

D. Storage and protection: The system components shall be stored and protected from exposure to harmful weather conditions and at temperature conditions as recommended by the manufacturer.

1.9 WARRANTY

A. General: The warranty period shall be for one (1) year period commencing with the System.

B. Acceptance date from the Owner.

C. Personnel: Warranty service shall be performed a technician who is trained and certified by the manufacturer.

D. Scope: The system supplier shall maintain a stock of replacement parts sufficient to provide responsive same-day or next-day service with a minimum of system "down" time.

1.10 TRAINING

A. Factory-trained personnel shall perform training.

B. Training shall include, but not limited to, system operation and system diagnostics.

1. Pre-installation: Database collection, design, and entry.
2. Post-installation: System operation including manual commands, database backup, system diagnostics, and history repeating.

PART 2 – PRODUCTS

2.1 SYSTEM PERFORMANCE

A. The Security Management System, hereinafter referred to as the System, shall be a modular and networkable access control system fully compatible with existing University of Delaware Security Management System. The system shall be capable of alarm monitoring, and control that allows for easy expansion or modification of inputs and remote control stations. The system control at a central computer location shall be under the control of a single software program and shall be provide full integration of all components. It shall be alterable at any time depending upon facility requirements. System reconfiguration shall be accomplished on-line through system programming.

B. Operating System shall match and be compatible with existing University of Delaware ProWatch Security Management System.

C. System software:

1. System operations- the following shall apply:

    a. Password: Operators shall be required to log on by entering a password.
    b. Information access: The system shall be capable of limiting operator access to sensitive information. Operators shall have proper authorization to edit the information.

D. Database audit log: The system shall be capable of creating an audit log in the history file following any change made to the system database by an operator. Each database item shall be selectable to audit the “add”, “update” or “delete” activities of related to that item. The system shall record:

1. The date and time of the activity.
2. The type of activity (add, update, or delete).
3. The user who performed the activity.
4. The workstation at which the activity took place.
5. What information was modified?
6. What the old value was.
7. What the new value was.

E. Operator log: The system shall be capable of creating an Action log in the history file following actions performed by an operator. The system shall record:

1. The date and time of the activity.
2. The user who performed the activity.
3. The workstation at which the activity took place.
4. What activity was performed?
5. What database item the activity was performed on.
6. What database group the item belongs to.

F. Alarm routing: The system shall be capable of defining routing groups that determine what information can be accessed by a user or class of users. Routing of alarms shall be separated via the following classifications:

1. The communication channels on which the alarm originates.
2. The type of alarms that are generated.
3. The workstations to which the alarm should be routed.

G. Badges: Shall maintain and be compatible with information related to the types of badges in use in the existing system software.

2.2 SECURITY MANAGEMENT FIELD CONTROLLERS

A. Access control field hardware devices: The security management system shall be equipped with access control field hardware required to receive alarms and administer all access granted/denied decisions. All field hardware shall meet UL requirements and be listed for intended purpose. The supported field hardware will include, but not limited to, the following components:

1. Intelligent controller (IC): An IC shall link the security management system software to all other field hardware components (card reader modules and input and output control modules). The IC shall provide full distributed processing of access control and alarm monitoring operations. Access levels, hardware configurations, and programmed alarm outputs assigned at the administration workstation shall be downloaded to the IC, which shall store the information, and function using its high-speed, local 32-bit microprocessor. All access granted/denied decisions shall be made at the IC to provide fast responses to card reader transaction. Manufacturer shall be NexWatch PW5K1IC.
    a. IC Networking: The system shall include a network-based interface module. The module shall be a 10 MBPS Ethernet-based and capable of residing on a local area network (LAN) or wide area network (WAN) without connectivity to a PC serial port. The IC network interface module shall be able to communicate back to the database server though industry standard switches and routers.

b. Off-line operation: In the event that the IC loses communication with system software, it shall continue to function normally (stand-alone). While in this off-line state, the IC shall make access granted/denied decisions and maintain a log of the events that occur. Events shall be stored in local memory and uploaded to the system software after communications are restored.

c. Features: The IC shall contain the following features:

i. Communications: The IC shall include a primary and a secondary port for the purpose of communication to the host computer. The following communication formats shall be supported:

- RS-232 at a speed of 38.4 KBPS
- RS-485 at a speed of 38.4 KBPS
- Ethernet at 10 MBPS (10baseT, RJ45)

ii. Memory: Real time program updates and overall host communications shall utilize flash memory. The IC shall support up to 100,000 cardholders and 50,000 event buffer.

iii. Additional ports: Shall be provided for connecting card readers and data gathering panels via RS-485 multi-drop wiring configuration. Three (4) ports shall be available with up to a combined total of 32 boards connected in any combination.

iv. Devices: Up to 32 devices consisting of reader interface modules, input modules (IM), and output modules (OM) shall be supported. The devices shall be connected in any combination.

v. Processor: The IC shall contain a 32-bit processor.

vi. Light emitting diodes (LED) shall indicate status of components and communication links.

vii. Readers: The IC shall support the following:

- Wiegand card formats and existing University of Delaware.
- Issue code support for Wiegand card readers.
- Up to 8 digit PIN codes.

viii. Electrical Power:

- Primary input power shall be 12VDC plus or minus 10 percent at 400mA with an operating range of 10 VDC to 16 VDC.
- The IC shall be equipped with an uninterruptible power supply (UPS) and backup battery sized to provide 24 hours of UPS power.

2. Single reader module (SRI): The SRI shall provide an interface between the IC and the card readers. The SRI shall operate with any card reader that produces a standard Wiegand (Data 1/Data 0 or Clock and Data) communication output. A single IC shall be able to multi-drop up to 32 SRIs. Manufacturer shall be NexWatch PW5K1R1 or PW6K1R1 for new installs. The following requirements shall also apply:

    a. Up to 32 SRIs shall be connected to each IC.
    b. Each SRI shall include two (2) relay inputs and two (2) relay outputs.
    c. Up to 8 unique card formats shall be supported.
    d. The SRI shall support an integrated card reader/keypad.
    e. The SRI shall support three (3) access modes upon loss of communication with the IC. These modes shall be locked, unlocked, or facility code.
    f. Input power shall be 12VDC plus or minus 10 percent at 400mA with an operating range of 10VDC to 16VDC.

3. Two reader module (DRI): The DRI shall provide an interface between the IC and the card readers. The DRI shall operate with any card reader that produces a standard Wiegand (Data 1/Data 0 or Clock and Data) communication output. A single IC shall be able to multi-drop up to 32 DRIs. Manufacturer shall be NexWatch PW5KxR2. The following requirements shall also apply:

    a. Each DRI shall support two card readers, each of which may be up to 500 feet from the DRI.
    b. Up to 32 DRIs shall be connected to each port on the IC.
    c. Each DRI shall include two (2) relay inputs and two (2) relay outputs per reader.
    d. Up to 8 unique card formats shall be supported.
    e. The DRI shall support an integrated card reader/keypad.
    f. The DRI shall support three (3) access modes upon loss of communication with the IC. These modes shall be locked, unlocked, or facility code.
    g. Input power shall be 12VDC plus or minus 10 percent at 400mA with an operating range of 10VDC to 16VDC.

4. Input module (IM): The IM shall monitor all system alarm inputs. The manufacturer shall be NexWatch PW5KxIN. The following requirements shall apply:

    a. The IM shall provide up to 16 supervised alarm inputs to monitor and report fault conditions (open, short, ground, or circuit fault) alarm conditions, power faults, and tampers. Upon alarm activation, the associated alarm condition shall be reported to the IC and subsequently to the system alarm monitoring workstation.
    b. Light emitting diodes (LED) shall indicate the status of the sixteen (16) alarm zones, cabinet tamper, and power fault.

c. The Input Modules shall operate independently and in conjunction with the Output Modules (OM), which shall send an output signal to a corresponding output device upon alarm activation. Upon alarm activation, the IM shall activate any or all alarm outputs within the OM. The OM shall provide Sixteen (16) Form C outputs rated at 5A @ 30VDC. Upon receipt of an alarm input from the IM, the OM shall transmit an activating signal to a corresponding output device.
d. Up to 32 IMs shall be connected to an available IC via RS-485 cabling.
e. Diagnostic light emitting diodes (LED) shall indicate IC communication, input zone scanning, and IM heartbeat.
f. The IM shall contain the following features:
    i. Alarm contact status scanning at up to 180 times per second for each zone.
    ii. Eight (8) configuration DIP switches to assign unit addresses and communications speed.
    iii. A low power CMOS microprocessor.
    iv. Filtered data for noise rejection to prevent false alarms.
    v. Two form C, 2A at 28VDC contacts for load switching.
    vi. Two dedicated inputs for tamper and power status.
    vii. Individual shunt times (ADA requirement).
g. Input power shall be 12VDC plus or minus 10 percent at 350mA with an operating range of 10VDC to 16VDC.

5. Output module (OM): The OM shall incorporate 16 output relays that are capable of controlling a corresponding output device upon any input activation or on command from the system.

    a. Output relays shall be capable of responding to:
        i. Input alarms from within the same IC.
        ii. Commands from a system operator.
        iii. Time zone control commands for automatic operation.
    b. Output relays shall be capable of:
        i. Pulsing for a predetermined duration that shall be programmable for each relay individually.
        ii. Following any input point an IM attached to the same IC (ON with alarm, OFF when clear, or as required).
        iii. Responding on command from the system operator to pulse, command on, command off, or reset to normal state.
    c. Each OM shall provide sixteen (16) Form C relays rated at 2A at 28VDC. The OM shall control the relays via digital communication. Upon receipt of input from the IM or command from the system operator, the IM will transmit an activating signal to the corresponding relay.
    d. Input power shall be 12VDC plus or minus 10 percent at 400mA with an operating range of 10VDC to 16VDC.

6. Card readers: Card readers and/or keypads shall be provided at the specified locations. These shall be installed at the height shown on the drawings. The cabling to the readers shall be shielded and grounded as per the manufacturer's instructions. Card readers shall be mounted 44" above finished floor to top of reader with LED at top. Care should be taken to avoid errant contact between the shield and doorframe. Any one, or a combination of the following components, shall be provided:
    a. Proximity card readers with Wiegand output: The reader style and finish shall be selected from the standard manufacturer's product list as shown on the installation documents be compatible with and match existing University readers.
        i. Power: The reader shall be powered by 5VDC or by the controller's internal 12VDC regulated power supply.
        ii. Mounting: The reader shall be capable of being mounted against metal door or window frames.
        iii. Range: The reader shall be capable of reading cards at a range of five to eight inches.
        iv. Card readers to be covered by signage identifying the building. All text for signs, including names and titles, will be prepared by the requestor and reviewed and approved by FP&C.

2.3 ENCLOSURE

A. Cabinet: The Controller enclosure shall be a NEMA Type 1 cabinet suitable for wall mounting, with knockouts. The cabinet shall have a hinged cover, tamper switch, and key lock.

1. Dimensions: The dimensions shall not exceed 18 inches in height, 14 inches in width, and 8.0 inches in depth.
2. Capacity: The enclosure shall hold up to nine (9) control modules, a power supply and a self-contained replaceable lead calcium backup battery.
3. All SDM door alarm boards to be mounted in a Hammond 1439R4 enclosure with lock to accept a Best core.

2.4 ELECTRICAL POWER REQUIREMENTS

A. System power: The system shall operate using standard 120VAC, 50/60-Hz power. The connection to the main building power supply shall be provided. This shall include connection to and provision of Uninterrupted Power Systems (UPS), capable of powering 25 percent lock load for 24 hours.

B. Enclosure power supply:

1. An inline transformer, rated at 12VDC, 4A continuous power shall provide power.
2. The power enclosure shall be provided with LED indicators showing normal operating conditions, loss of AC power-standby battery supplying power, loss of AC power, discharged or no standby battery, and no DC output.
3. The enclosure shall include a 12VDC, sealed lead calcium battery, securely fastened to the enclosure to prevent the accidental removal of the battery. It shall be capable of providing backup for 24 hours depending on module configuration.
4. 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.
5. Backup power supply capacity: 24 hours of battery supply. Submit battery and charger calculations size backup batteries for 125 percent of amp-hour standby requirement.

2.5 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.

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.

2.6 ENVIRONMENTAL CONDITIONS

A. Environmental conditions: The system shall be designed to meet the following environmental conditions:

1. Storage temperature: The system shall be designed for a storage temperature of -10 degrees C to 70 degrees C.
2. Operating temperature: The system shall be designed for an operating temperature of 2 degrees C to 43 degrees C.
3. Humidity: The system shall be designed for normal operation in an 85 percent relative humidity, non-condensing environment.
4. Electromagnetic interference: The system shall meet or exceed the requirements of FCC Part 15, Class B devices, FCC Part 68, IEC EMC directive.

2.7 ASSOCIATED EQUIPMENT

A. The System shall be compatible with existing University of Delaware cards using University of Delaware's unique facility code (HID Corporate 1000 35-bit card format).

2.8 CARD READERS

A. Acceptable manufacturer: Ingersoll Rand, Model AptiQ multi-technology reader, or approved equal.

B. Power: Card reader shall be powered from its associated Controller, including its standby power source.

C. Response time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be 800 milliseconds or less, from the time the card reader finishes reading the credential card until a response signal is generated.

1. Card readers to be covered by signage identifying the building. All text for signs, including names and titles, will be prepared by the requestor and reviewed and approved by FP&C.

D. Enclosure: Suitable for surface, semi-flush, or pedestal mounting. Mounting types shall additionally be suitable for installation in the following locations:

1. Indoors, controlled environment.
2. Indoors, uncontrolled environment.
3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as need for operation at the site.

E. Display: LED or other type of visual indicator display shall provide visual and audible status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

F. Proximity readers:

1. Card readers shall provide power to compatible credential cards, and shall receive and decode a unique identification code number transmitted from the credential card.
2. The card reader shall read proximity cards in a range from contact with to at least 6 inches from the reader.
3. Card reader data output shall be Wiegand format compatible with existing University system.

2.9 ELECTRIC LOCK

A. Electric strikes to be Folger Adam 310-4 with rim exit device or Folger Adam 310-2 with mortise lock using hex head mounting bolts only.

B. All electric strikes to have LBM and LCM option.

C. Residential Halls to have tamper switch to indicate removal of electric strike. GRI PB-100 or GRI PB-2020.

D. All electric strikes to have surge suppression installed per Honeywell guidelines.

E. A tamper switch must be installed on latch when an electric strike is not installed.

2.10 DOOR POSITION SWITCH (DOOR CONTACT)

A. Acceptable manufacturer: Flair Electronics, Model MSS200-7 recessed balanced magnetic switch, or approved equal.

B. In cases where 2 doors are wired to one SDM 100 one door to use MSS200-7 and other door to use PFC48Y door contact.

C. The door position switch shall detect a one inch of separating relative movement between the magnet and the switch housing. Upon detecting such movement, the Door Position Switch shall transmit an alarm signal to the security management system.

D. The door position switch shall consist of a switch assembly and an actuating magnet assembly. The magnet shall be of the rare earth type. Switches shall be rated for a minimum lifetime of 1,000,000 operations. The magnet assembly shall house the actuating magnet.

E. Door Position switches to be mounted wood, construction foam is not allowed.

F. Door contacts to be glued in place to prevent tampering or removal.

2.11 LOCAL ALARM HORN

A. Commercial applications; Provide flush mounted, white in color, mini-horn suitable for mounting to a flush mounted single gang electrical work box. Match local alarm horn voltage requirements with security management system power supply output. Horn shall provide a steady audible output of 87 dB at 10 feet. In/out screw terminals shall be provided suitable for number 12 AWG to 18 AWG conductors.

B. Residential applications; Revere Siren RVL-18C/SRN-SC.

2.12 ISOLATION RELAY

A. Acceptable manufacturer: Altronix relay module, Model RBST, or approved equal to be installed on all motorized door openers.

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 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.

D. The Security Management System shall be installed in accordance with all local codes and manufacturer's recommendations.

3.2 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; 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 holiday, 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 Fire Alarm System features.
7. Prepare and install all required software and data files, alarm graphic maps at University Central Station Monitoring Location.
8. Develop user-defined fields.

9. Develop screen layout formats.
10. Complete system diagnostics and operation verification.
11. Prepare a specific plan for system testing, startup, and demonstration.
12. Develop acceptance test concept and, on approval, develop specifics of the test.
13. Develop cable and asset management system details; input data from construction documents. Include system schematics and As-built Drawings.

D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents and provide set up of system software. Provide all specific project data file input to the system project.

3.3 CABLING

A.
1. Comply with NECA 1, "Good Workmanship in Electrical Contracting."
2. Install cables and wiring according to requirements in Division 16 Sections.
3. Wiring Method: Install wiring in raceway except within consoles, cabinets, desks, and counters. Conceal raceway and wiring above suspended ceiling sand inside walls except in unfinished spaces.
4. Wiring Method: Install wiring in raceway except within consoles, cabinets, desks, and counters. Use NRTL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway except in unfinished spaces.
5. Install LAN cables using techniques, practices, and methods that are consistent with Category 5E rating of components and that ensure Category 5E performance of completed and linked signal paths, end to end.
6. Install cables without damaging conductors, shield, or jacket. Terminate shields as recommended by equipment manufacturer.
7. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees residents 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 employee residents or the public shall be covered with a suitable cover plate and secured with tamperproof screws.
8. Install end-of-line resistors at the field device location and not at the Controller or panel location.

3.4 CABLE APPLICATION

A. Comply with EIA/TIA-569, "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. RS-232 Cabling: Install at a maximum distance of 25 feet 24 AWG conductors.

D. RS-485 Cabling: Install at a maximum distance of 4000 feet 24 AWG, 2 twisted pairs, shielded (Belden 9842 or equivalent).

E. Card readers and input/output circuits.

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 18 AWG wire.
3. For greater distances, increase conductor size or provide “repeater” modules recommended by manufacturer of the Controller.
4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50mA or more.

F. Install minimum No. 16 AWG cable from Controller to electrically powered locks provide conductor size in accordance with manufacturer’s recommendations.

3.5 GROUNDING

A. Comply with Division 16 Section "Grounding and Bonding."

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

E. 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.

3.6 INSTALLATION

A. Provide isolation relay between the intelligent controller (IC) and automatic motorized door operator. : Altronix relay module, Model RBST

B. Push buttons: Push buttons shall be mounted 42 inches above finished floor. Push-button switches shall be connected to the Controller associated with the portal to which they are applied, and shall operate the appropriate electric strike, electric bolt, or other facility release device.

C. Install card, fob, and biometric readers at 42 inches above finished floor.

D. Mount horns at 7 feet 6 inches above finished floor.

3.7 IDENTIFICATION

A. In addition to requirements in this Article, comply with applicable requirements in Division 16 Section "Identification for Electrical Systems" and with TIA/EIA-606.

B. Provide 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, as-built drawings shall reflect as-built conditions.

3.8 SYSTEM SOFTWARE

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

3.9 FIELD QUALITY 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. Testing agency: Perform field tests and inspections and prepare test reports.

C. 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. Battery back up to last 24 hours minimum.
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 form each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

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

3.10 STARTUP SERVICE

A. Engage a factory-authorized service representative to supervise and assist with startup service. Complete installation and startup checks according to approved procedures that were developed in "PREPARATION" Article and with manufacturer's written instructions.

1. Enter Building specific programming and data files for Owner's operators, management, and security personnel.

3.11 TESTING AND CERTIFICATION

A. The access control and alarm monitoring shall be tested in accordance with the following:

1. The Contractor shall conduct a complete inspection and test of all installed access control and security monitoring equipment. This includes testing and verifying connection to equipment of other Divisions, such as Life Safety and Elevators.
2. The Contractor shall provide staff and equipment to test all devices and all operational features of the system for witness by the Owner's representative and the Authority having jurisdiction. The Owner's representative prior to acceptance must witness all testing.
3. The testing and certification shall take place as follows:

    a. System shall be tested in conjunction with the manufacturer's representative.
    b. All deficiencies noted in the above test shall be corrected.
    c. System test witnessed by Owner's representative and Electronic Shop manager or designee correction of any deficiencies noted.
    d. The Owner's representative shall accept the system.
    e. The Authority having jurisdiction shall witness system test. Any deficiencies noted shall be corrected.

4. A letter of certification shall be provided to indicate that the tests have been performed and all devices are operational.

3.12 DEMONSTRATION

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

End of Section