DIV 28 – SAFETY AND SECURITY SYSTEMS TABLE OF CONTENTS

SECTION	TITLE	PAGES
28 0500	Electronic Safety and Security	7
28 1000	Electronic Access Control and Intrusion Detection	7

SECTION 28 0500

ELECTRONIC SAFETY AND SECURITY

PART 1 - GENERAL

1.1 SCOPE

A. Perform all Work required to provide and install the electronic safety and security indicated by the Contract Documents with supplementary items necessary for proper installation.

1.2 REFERENCES

A. The latest published edition of a reference shall be applicable to this Project unless identified by a specific edition date.

B. All reference amendments adopted prior to the effective date of this Contract shall be applicable to this Project.

C. All materials, installation and workmanship shall comply with the applicable requirements and standards addressed within the Contract Documents.

1.3 SUBMITTALS

A. General

1. All submitted data shall be specific to this project and identified as such. Generic submittal data will not be accepted.

2. Submit transformer and amplifier locations for review.

B. Product Data

1. Manufacturers descriptive literature, illustrations and installation instructions for all components included within this project indicating compliance with applicable referenced standards, size, dimensions, model number, electrical characteristics, support requirements, connection requirements and all applicable information verifying that submitted components comply with Contract Documents.

C. Record Documents

1. Identify transformer and amplifier locations on the record drawings.

2. Manufacturer's warranty form in which manufacturer agrees to repair or replace components which fail in materials or workmanship within specified warranty period.

D. Operation and Maintenance Data

1. Operation Data: Include manufacturer’s installation and operating instructions.

2. Maintenance Data: Servicing requirements, inspection data, preventative maintenance schedule, exploded assembly views, replacement part numbers and availability, location and contact numbers of service depot.

E. LAN/WAN Network Devices

1. All LAN/WAN Networked Devices shall require an additional submittal to identify the MAC Address of the Contractor provided device, the location to be installed and the port configuration needed for communication. The expected turn-around time for this data to be provided back to the contractor is three (3) weeks.

1.4 QUALITY ASSURANCE

A. Product Standards

1. All materials installed on this or any other project must be new and the latest specification and version from the manufacturer.

2. All products installed shall be what is depicted in these specifications with no exceptions.

1.5 RELATED DOCUMENTS

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

B. Specifications throughout all Divisions of the Project Manual are directly applicable to this Section, and this Section is directly applicable to them.

1.6 SUMMARY

A. Provide all work as detailed in the Contract Drawings as a turn-key installation including all material, labor, programming, as-built documentation, warranties, taxes, freight and permits. Only items and requirements specifically stated to be provided under another section shall not be a requirement for this section of the work.

B. The end product by which the security contractor is to produce shall be a complete, operational and functional integrated security system.

C. Systems and Equipment

1. Provide the following systems and equipment:

a. Security Management System (SMS)

b. Wire and Cable

D. Coordination

1. Coordinate all installation of the security system with the following related systems:

a. Door Hardware

1.7 DELIVERY, STORAGE AND HANDLING

A. Equipment and components shall arrive on-Site properly protected and undamaged with containers, packaging and labels intact.

B. Store, handle and protect materials and equipment in accordance with Manufacturer's recommendations.

C. Provide additional protection during handling as necessary to prevent breaking scraping, marring, or otherwise damaging products or surrounding areas.

D. Protect all equipment and components that are to be installed within this project from theft, vandalism, and exposure to rain, freezing temperatures and direct sunlight.

E. Protect installed equipment and components from damage and prevent use by unauthorized persons.

1.8 WARRANTY

A. Warranty

1. The Contractor shall warranty the completed work for a period of one (1) years, from the date of system acceptance, to be free of defect in design, workmanship or material.

2. System acceptance is defined as the completion of all functional performance testing and the resolution of all punch list items.

B. Warranty Service

1. In the event that defects in the materials and/or workmanship are identified during the warranty period, the contractor shall provide all labor and materials to correct the deficiency.

2. All service work shall be performed by factory certified technicians.

3. All warranty service shall include the replacement of all parts and or components as required to restore normal system operation. If parts or components need to be repaired, a loaner will be supplied and installed until the part or component can be repaired and reinstalled.

4. Immediately following a warranty service request, the Contractor shall provide written documentation to the Owner which details the service work completed, cause of trouble and any outstanding work required to restore a complete and normal system.

C. Repair and/or Replacement Service

1. Service shall be completed within two (2) schedules dependent on criticality:

a. Schedule One – seven (7) days a week 24 hours a day

b. Schedule Two – 8am to 5pm on business days

D. Schedule One shall apply to major system components

E. All Repairs shall be completed within 48 hours from site arrival. If the failure exceeds 48 hours, reserves the right to require the contractor to provide on-site manufacturer support at no additional cost to the Owner.

F. The Owner reserves the right to expand or add to the system during the warranty period using firms other than the Contractor for such expansion without affecting the contractor's responsibilities, provided that the firms used are authorized dealers for the equipment or system being expanded.

PART 2 - PRODUCTS

2.1 GENERAL

A. All materials shall meet or exceed all applicable referenced standards, federal, state and local requirements, and conform to codes and ordinances of authorities having jurisdiction.

2.2 ACCESS CONTROL

A. Doors control

1. Remote control of doors.

2. Control point outputs for lock power and device control activated by a card reader or SMS.

3. The SMS shall allow button selection for five (5) seconds per valid card read.

4. When the card reader is in free access the hall call buttons shall operate normally.

2.3 WIRE AND CABLE

A. Minimum Specifications

1. All wire and cable shall be Underwriter's Laboratories (UL) approved for its intended application, shall meet all national, state and local code requirements for its application, and shall meet or exceed manufacturers' recommendations for the components connected.

2. Provide Plenum-rated cable as required by code.

3. All wire and cable shall meet individual system or subsystem manufacturer specifications. All cabling shall be in accordance with the PDS standards set in place by MD Anderson.

4. Wire and cable shall comply with the applicable requirements of the National Electrical Code (NEC), latest edition, in regards to cable construction and usage.

5. Insulation shall be rated for a minimum of 300 volts

6. Patch Cables

a. All patch cables shall be pre-manufactured.

b. The length of all patch cables shall be long enough to route neatly through cable management systems and to be dressed in neatly.

c. All patch cables shall have owner standard ends.

B. Minimum Wire Types and Sizes

1. Low Voltage Power Cable

a. 18AWG, twisted, stranded, insulated, and jacketed

b. Increase conductor gauge to be consistent with circuit current ratings and manufacturer's recommendations.

2. Control Point Cable (Non-power)

a. 20 AWG, twisted, stranded, insulated, and jacketed

3. Control Point Cable (Low Voltage Power)

a. 18 AWG, twisted, stranded, insulated, and jacketed

4. Composite Cable

a. All Composite cable shall meet all of the above requirements. There shall not be a drain that is over the entire composite cable bundle, it shall be limited to the reader cable only.

1) West Penn Wire

2) Or Owner approved equivalent

PART 3 - EXECUTION

3.1 INSTALLATION

A. Installation shall meet or exceed all applicable federal, state and local requirements, referenced standards and conform to codes and ordinances of authorities having jurisdiction.

B. All installation shall be in accordance with manufacturer's specifications and published recommendations.

C. Wiring

1. Run wire with conduit, exposed above accessible ceilings, below accessible floors, in floor cable trays and in riser rooms.

2. Utilize cable trays whenever possible.

3. All cabling shall be installed per Owner's requirements.

4. All wireways shall be per construction documents. If the construction documents do not detail a wireway, it is the responsibility of the security contractor to provide their own wireway.

5. Provide plenum cable when ran thru Plenum areas.

6. Fasten cables throughout cable paths securely to building structure every 10 feet at minimum.

7. Cable runs shall be continuous from device location to the final point of termination.

8. Provide grommets and strain relief material where necessary to avoid abrasion of wire and excess tension on wire and cable.

9. Component Connections

   a. The following components must be labeled utilizing an approved labeling device with the above mentioned device naming standards:

   b. Card Readers – Both in the field and in the panel where it terminates. Field Labeling shall be affixed to the bottom, if not applicable on the inside edge, of each device.

   c. Cameras – Both in the field and where it terminates. Field Labeling shall be affixed to the camera above the ceiling, if not applicable the top edge of housing.

   d. All other previously listed security devices shall be labeled on the cable where it terminates to the device and where the cable terminates to the security controller or power supply.

   e. Prepare wire ends for attachment to components in accordance with manufacturer recommendations.

   f. Wire nuts shall not be an acceptable means of connecting wire and cable. All connections shall be made by crimp connection only.

   g. Connections shall be labeled with the above mentioned device naming standards.

   h. Controller Connections

   i. Contractor shall not connect any Istar controller to the SMS outside of the Owner's Technical Services Component's normal business hours. All initial system activations shall be performed and tested prior to implementation on the production environment.

D. Conduit

1. Exposed Outdoor Locations: Rigid steel conduit.

2. Concealed Dry Interior Locations: Rigid steel conduit

3. Exposed Dry Interior Locations: Rigid steel conduit

3.2 SYSTEM ACCEPTANCE

A. Functional Performance Testing (FPT) requires that an authorized representative of the Owner review all security technology components to assure they are properly installed, functional, and integrated into the Owner's existing security technology infrastructure.

B. Punchlist is developed and distributed by the Owner.

1. The Contractor shall produce documentation to demonstrate the punchlist has been completed and the installation is at Final Completion.

C. Once the system is accepted, the devices are then placed in the view of the Owner's Communication Center for monitoring and dispatch. Once system acceptance has been established by the Owner, that date will be the beginning of the warranty period.

D. The Owner reserves the right to suspend and/or terminate testing at any time when the system fails to perform as specified.

2.END OF SECTION

SECTION 281000 – ELECTRONIC ACCESS CONTROL AND INTRUSION DETECTION

PART 1 - GENERAL

1.1 SCOPE

A. Perform all work required to provide and install the electronic safety and security indicated by the Contract Documents with supplementary items necessary for proper installation.

B. Equipment included in this section

1. Access Control System

1.2 REFERENCE STANDARDS AND CODES

A. International Organization for Standardization (ISO)

1. 9001:2000 – Quality Management Systems.

B. Federal Communications Commission

1. Class A digital device, pursuant to Part 15 Frequency Devices.

1.3 DEFINITIONS

A. Access Control System: Comprises a PC Based Host, Access Control Software, Access Controllers and/or Access Control Devices.

B. Access Control Software: Usually contains tools for:

1. Data acquisition and change

2. Access Card Enrollment

3. The control of its own system components

C. Access Controllers: Machine aided control of access rights and the granting or denying of physical access.

D. Access Control Devices: Refers to doors and readers, and other opening door elements and sensors.

1.4 SYSTEM DESCRIPTION

A. Access Control System

B. Performance Requirements:

1. Control up to two (2) access readers per controller, system expandable to 1000 controllers.

2. Support Windows 10

3. Supports both standalone and client-server modes of operation.

4. Supports 802.3 or 802.11 b/g communications to the controller from host PC.

1.5 DELIVERY, STORAGE AND HANDLING

A. Deliver materials in manufacturer's original, unopened, undamaged containers; and unharmed original identification labels.

B. Protect store materials from environmental and temperature conditions following manufacturer's instructions.

C. Handle and operate products and systems according to manufacturer's instructions.

1.6 WARRANTY

A. Provide manufacturer's warranty covering one (1) year for the software and one (1) years warranty on Access Control Products to repair and replace defective equipment.

B. Exchanges available for product failures.

1.7 MAINTENANCE

A. Make ordering of new equipment for expansions, replacements and spare parts available to dealers or end users.

B. Provide factory direct technical support from 8:00 a.m. to 8:00 p.m. CST via phone and e-mail.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Basis of Design: Avigilon or approved equal

B. Substitutions:

1. All proposed substitutions must be approved by the Architect or Engineer professional.

2. Proposed substitutions must provide a line-by-line compliance documentation.

2.2 GENERAL

A. The Avigilon software shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tier software architecture.

1. The network appliance shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network-connected PC with a browser.

2. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.

3. Security of the data communicated over the network to and from the browser, Network Controller, and nodes is protected by encryption (SSL 128-bit) or authentication (SHA-1).
   a. Temperature Blade: shall support eight analog temperature sensor inputs.

B. The Avigilon system shall integrate, within a browser interface, access control, alarm monitoring, video monitoring, and temperature monitoring applications.

C. All equipment and materials used shall be standard components, regularly manufactured, and regularly utilized in the manufacturer's system.

D. All Avigilon systems and components shall have been thoroughly tested and proven in actual use.

E. All Avigilon systems and components shall be provided with an explicit manufacturer warranty of one year for software and two years for hardware.

2.3 HARDWARE REQUIREMENTS

A. Network-based Camera and Video Surveillance: The system shall provide live IP video surveillance capability. The number of supported cameras shall be limited only by license. The system's video capabilities shall include video monitor switching based on access activity. The system shall provide monitoring, configuration, and administration of IP video. Cameras can be separately monitored or monitored in groups.

1. Presets: The system shall support the creation, deletion, and editing of camera preset positions in the system. It shall also be possible to save changes in preset positions directly to a camera website.

2. Views: The system shall support the creation, deletion, and editing of multiple camera views, specifically Quad views (four cameras). The application shall provide a drop down pick list for selecting current views or naming of new views.

B. Access Control

1. The system shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs.

2. Time Specifications: The system shall be capable of storing up to 512 time specifications. Each time specification must be assigned a unique alphanumeric name of up to 64 characters. The definition of a time specification shall require the assignment of both a start time and end time. Each day of the week shall be individually assignable for inclusion in time specifications. Up to three holiday groups shall be assignable for inclusion in time specifications. If no holidays are assigned to a time specification then no holiday access shall be allowed.
   a. Time specifications shall be assignable to access levels, output groups, portal groups, input groups, and alarm events.

b. Time specifications shall function appropriately per node for the time zone specified for that node.

3. Access Levels: The system shall be capable of storing up to 512 access levels in each partition. Each access level must be assigned a unique alphanumeric name of up to 64 characters. The definition of an access level shall require the assignment of a reader or reader group, and a time specification. It shall be possible to also assign an elevator floor group to an access level.

4. First-in Unlock Rule: The system shall support the use of a First-in unlock rule. It shall be possible to use this rule to control the unlock behavior of portal groups with assigned unlock time specs.

   a. The First-in unlock rule shall require a card read of a specified access level. The portals in the group shall unlock only when the rule is satisfied and the unlock time spec is valid.
   b. There can be up to 64 First-in unlock rules in the system at a time.

5. Holidays: The system shall be capable of storing up to 30 holidays per partition. Each holiday must be assigned a unique alphanumeric name of up to 64 characters. The definition of a holiday shall require a start date and an end date. Holidays shall have the ability to span several days using only one holiday slot. Holiday definitions shall support the designation of a start time and an end time. If no start time is designated the the system shall default to 00:00 (start-of-day). If no end time is designated then the system shall default to 24:00 (end-of-day). Holidays shall require the use of 24-hour time format, e.g. 17:00 is 5:00 PM.

6. Two-man entry restriction: It shall be possible to require two (2) valid card reads by different cardholders within a specified number of seconds for entry to a specific portal.

7. Anti-passback: The system shall support both regional and time anti-passback access control. For anti-passback functions, it shall be possible to configure regions, assign readers to those regions, and specify events for response to tailgate, passback, and occupancy limit violations. It shall also be possible to designate parent regions for hierarchial anti-passback.

   a. Grace: It shall be possible for a system Monitor or Administrator to Grace card holders from passback and tailgate violations.
   b. It shall also be possible to set a specific time for all cardholders to be Graced daily.
   c. The system shall be able to automatically place the cardholder in a predefined region upon the selection of the grace option.

8. Mustering: To aid in evacuation management it shall be possible to designate a region or regions for mustering. It shall be possible to quickly get an occupancy count and occupant list for any region.

9. Scheduled Actions: It shall be possible to specify system actions to occur at scheduled times. When scheduling an action, it shall be possible to specify whether the time specifications for the scheduled action will be based on the time zone set for the local Network Node or the time zone set for the Network Controller. Scheduled actions can include:

   a. Arming and disarming inputs.
   b. Activating and deactivating outputs.
   c. Locking and unlocking portals.

10. Floor plans: The system shall be capable of displaying active graphic floor plans and configuring each floor plan with icons representing system resources: cameras, portals, temperature points, and alarms. A network administrator holding at least a 'Setup' user role shall be able to upload floor plan images and graphically configure device icons onto the floor plan images. Viewing floor plans will require the Macromedia Flash Player 9.0 plug-in for the browser.

    a. It shall be possible to create floor plan groups for the purpose of assigning or withholding assignment of these groups to system user permissions know as Custom User Roles. If a floor plan group is assigned to a particular system user then the floor plans in that group shall be viewable by that system user.
    b. The Configuration page lets users configure the destination entry server (DES) nodes, destination entry director (DER) nodes, and destination entry computer (DEC) nodes in the Compass system.
    c. The Events page lets users view the IP address, name, node type, and status of each node in the Compass system.
    d. The Reader Groups and Access Levels pages let users configure reader groups and their associated access levels within the Compass system.

    e. Wire and program card reader LEDs to indicate the conditions and functions as follows:
        1) RED LED in the normal locked state
        2) GREEN LED upon a valid card read and the door is in the unlocked mode
        3) Flashing RED LED upon an invalid card read, forced door and held open door alarm conditions.
        4) Card Readers LEDs shall operate identically throughout the project.

11. Fire alarm system: The system shall receive signal from the Fire Alarm panel for automatic egress upon alarm.

C. Door Position Switches

1. Normally Closed door position switches

2. Acceptable Manufacturer

    a. Sentrol 1078 – Basis of Design
    b. Or approved equal to

D. Power Supplies

1. Provide power supplies for all SMS equipment. Contractor to size accordingly.

2. The power supply for the SMS equipment shall have a minimum four (4) hour backup and shall not be shared with any other security device.

3. Acceptable Manufacturer

    a. Electronic Security Devices
    b. Offline
    c. Switching Power Supplies with Battery Chargers
    d. Or approved equal to

4. Provide power for all electric locking mechanisms except Delayed Egress Locking Devices and Electric Latch Retraction Devices.

5. All PDUs controlling security devices and other readers, shall be 24 Volts DC.

6. Fail Secure Locks shall operate normally upon fire alarm activation and during power failure conditions.

7. Fail Safe Locks shall unlock under the following conditions:

    a. Building Fire Alarm

    b. Loss of Panel Power

    c. Failure of the Power Supply

8. Provide Power Distribution boards with independent fused outputs and relays for all locking hardware. Power distribution boards for fail safe locks shall include a fire override relay. Interface the relay with the fire alarm system such that a dry contact from the fire alarm system shall remove power to all fail safe devices during a fire alarm condition.

9. Provide power supplies with independent fused outputs for all other security devices (i.e. local alarm panels, motions). There shall be no bussing of any device requiring power.

10. Acceptable Manufacturers

    a. BASE electronics
    b. Alarm-Saf
    c. Or UTPD approved equivalent

2.4 CERTIFICATIONS

A. UL 294 listed.

B. ISO 9000 listed.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Examine areas to receive devices and notify adverse conditions affecting installation or subsequent operation.

B. Do not begin installation until unacceptable conditions are corrected.

3.2 PREPARATION

A. Protect devices from damage during construction.

3.3 INSTALLATION

A. Install controllers and devices in accordance with manufacturer's instructions at locations indicated on the floor drawings plans.

B. Ensure selected location is secure and offers protection from accidental damage

C. Location must provide reasonable temperature and humidity conditions, free from sources of electrical and electromagnetic interference.

D. Ensure power source is protected against accidental shutoff.

3.4 FIELD QUALITY CONTROL

A. Test snugness of all terminal strip mounting screws.

B. Test proper operation of controllers and readers per the manufacturers commissioning document. Present card to the readers to validate if reader functions correctly.

C. Determine and report all problems to the manufacturer’s customer service department.

3.5 ADJUSTING

A. Make proper adjustment to controller, extensions and readers for correct operation in accordance with manufacturer’s instructions.

3.6 DEMONSTRATION

A. Demonstrate at final inspection that access control system and devices functions properly.

END OF SECTION 280500