SECTION 28 15 00 - ACCESS CONTROL SYSTEM

PART 1 - GENERAL

1.1 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. This work shall be done in strict accordance with these Contract Documents prepared for The Pennsylvania State University, hereafter referred to as "Owner".

C. The Contractor shall perform all work described in this document along with any work not expressly mentioned in the specifications, but obviously necessary for the proper execution of the same. It is not the intent to delineate or describe every detail and feature of work. No additions to the contract sum will be approved for any materials, equipment, and/or labor to perform work hereunder unless it can be clearly shown to be beyond the scope and intent of the drawings and specifications and absolutely essential to the proper prosecution of the work.

D. Work under this contract consists of the complete installation and includes, but is not necessarily limited to, the furnishing of all labor, superintendence, material, tools, and equipment necessary to complete all the work as specified herein.

1.2 SUMMARY

A. Section Includes:

1. Access Control System Components
2. Cables
3. Transformers

B. Related Requirements:

1. Door Details: Refer to Contract Documents.

C. Owner Requirements:

1. Furnish, install, and program a functionally complete integrated access control, electronic locking, and door monitoring system per Manufacturer's guidelines and codes, as described in these specifications.
2. Equipment and application shall comply with PSU Policy AD-65.

1.3 DEFINITIONS

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

B. DTS: Digital Termination Service. A microwave-based, line-of-sight communication provided directly to the end user.

C. 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.

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

E. PC: Personal computer. Applies to the central station, workstations, and file servers.

F. RAS: Remote access services.

G. RF: Radio frequency.

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

I. TCP/IP: Transport control protocol/Internet protocol.

J. TWAIN: Technology Without An Interesting Name. A programming interface that lets a graphics application, such as an image editing program or desktop publishing program, activate a scanner, frame grabber, or other image-capturing device.

K. WMP: Windows media player.

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

M. WYSIWYG: What You See Is What You Get. Text and graphics appear on the screen the same as they will in print.

1.4 ACTION SUBMITTALS

A. Product Data: Specification sheet for each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a location on Drawings.

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

1. Diagrams for cable management system.
2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Parts 2 and 3.
3. Wiring Diagrams. For power, signal, and control wiring. Show typical wiring schematics including the following:

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

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

C. Product Schedules: Identify model number, quantity, and unit cost of each device.

D. Permits: Identify requirements for permits from all building, police, and fire authorities for the installation of the specified system(s). Assist the Owner in obtaining the required permits.

E. Specification Compliance: Provide a letter with the bid indicating compliance with the specifications, referencing each sub-section individually. List any exceptions, substitutions, or alternatives to each sub-section as appropriate. Requests for substitutions shall be submitted to the Engineer, along with all relevant technical data pertaining to substituted equipment, ten (10) days prior to the close of bid for evaluation and approval.

1.5 INFORMATIONAL SUBMITTALS

A. Field quality-control reports.

1.6 CLOSEOUT SUBMITTALS

A. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals. In addition to items specified in Section 01 78 23 "Operation and Maintenance Data," include the following:

1. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on USB media of the hard-copy submittal.
2. System installation and setup guides with data forms to plan and record options and setup decisions.

B. As-Built Drawings: PDF files generated from either AutoCAD or Revit of each floor plan.

1. Indicate exact device locations, panel terminations, cable routes, and wire numbers as tagged and color-coded on the cable tag.
2. Provide final point-to-point wiring diagrams of each type of device.
3. Provide to Owner for approval prior to final system acceptance walk through.

C. Hard copies of the following shall be placed in each iSTAR panel installed on this project:

1. iSTAR installation manual.
2. Reader and reader interface manual(s).
3. Door release hardware manual(s).
4. Request to exit motion detector manual(s).
5. Power supply manual(s).
6. All wiring notes.

1.7 QUALITY ASSURANCE

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

1. Cable installer must have on staff an RCDD certified by Building Industry Consulting Service International.
2. Contractor shall be a factory-authorized and trained dealer of the system and shall be certified to maintain and repair the system after system acceptance.

B. Source Limitations: Obtain central station, workstations, controllers, Identifier readers, and all software through one source from single manufacturer. Manufacturer shall have been in business manufacturing similar products for at least five (5) years.

C. All equipment, systems, and materials furnished and installed under this section shall be installed in accordance with the applicable standards of:

1. National Fire Protection Association (NFPA)
2. National Electric Code (NEC, NFPA 70)
3. Underwriters Laboratories (UL)
4. Pennsylvania Department of Labor and Industry (L&I)
5. EIA/TIA Telecommunications Wiring Standards
6. Local authorities having jurisdiction (AHJ)
7. The Pennsylvania State University (PSU)

D. All components, parts, and assemblies supplied by the Manufacturer and installed by the contractor shall be warranted against defects in material and workmanship for a period of at least twelve (12) months (parts and labor), commencing upon date of acceptance by Owner. A qualified factory-trained service representative shall provide warranty service.

1.8 DELIVERY, STORAGE, AND HANDLING

A. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 deg F, and not more than 80 percent relative humidity, noncondensing.

B. 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.

C. Mark packing list with the same designations assigned to materials and equipment for recording in the system labeling schedules that are generated by software specified in "Cable and Asset Management Software" Article.

D. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.9 PROJECT CONDITIONS

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

1. Control Station: Rated for continuous operation in ambient conditions of 60 to 85 deg F and a relative humidity of 20 to 80 percent, noncondensing.
2. Indoor, Controlled Environment: NEMA 250, Type 1 enclosure. System components, except the central-station control unit, installed in temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of 36 to 122 deg F dry bulb and 20 to 90 percent relative humidity, noncondensing.

3. Outdoor Environment: NEMA 250, NEMA 250, Type 3R enclosures. System components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of minus 30 to plus 122 deg F dry bulb and 20 to 90 percent relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 85 mph and snow cover up to 24 inches thick.

PART 2 - PRODUCTS

2.1 OPERATION

A. Security access system hardware shall use a single database for access-control and credential-creation functions.

2.2 PERFORMANCE REQUIREMENTS

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

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

C. Comply with SIA DC-03.

2.3 ACCESS CONTROL SYSTEM

A. Description: The Pennsylvania State University has initiated a multi-phase access control project for the University Park and Commonwealth campuses. The system utilizes Tyco Software House CCure9000 software running on a CCure server. The hardware consists of Tyco Software House iSTAR Controller and associated hardware, which provides for the physical connection to readers, locking hardware, door status switches, and request to exit devices.

Software House iSTAR has been approved as a Proprietary Item and substitutions will not be permitted without permission of Owner.

B. Software House iSTAR System Feature/Capability: The following indicates system capabilities and capacities:

1. LAN/WAN Communications: CCure host server to local iSTAR panel.
2. The iSTAR panels shall have a minimum of 64MB RAM to exceed the University requirement of 10,000 card records and 3,000 event storage capabilities to retain event information in the case of network failure.
3. Programming Software: The programming software shall include the following features:

    a. LAN/WAN connection with CCure Host
    b. Fully configurable user authority level control
    c. CCure parameter editing and storage
    d. CCure and iSTAR software upgrade ability
    e. LAN/WAN Communications database management
    f. Event history buffer uploading

C. Software House iSTAR System Interface Requirements

1. All Installations: The Software House iSTAR access control system shall be installed in accordance with the National Electric Code and the local Authority Having Jurisdiction (AHJ).
2. The Software House iSTAR access control hardware shall be installed in accordance with UL requirements.

2.4 SYSTEM MATERIALS

A. System Hardware Description

1. iSTAR System: The access control system shall be provided, at a minimum, with the following components. Additional accessories shall be provided based on the quantities and features required for the application.

a. Tyco Software House iSTAR panel.

1) System Accessories:

a) 64 MB RAM or greater
b) iSTAR power supply with 7 amp hour battery backup for panel and door strikes

b. HID Signo series card readers
c. Software House RM-4 reader module
d. Von Duprin PS873 power supplies for electric latch retraction activation
e. Von Duprin exit hardware mounted request-to-exit switches
f. Von Duprin electric latch retraction solenoids
g. Von Duprin 6000 Series electric door strikes
h. Interlogix 1078C door status monitor switches
i. Bosch Security Systems DS160 request-to-exit motion detectors with integral sounders
j. System Sensor PA400 Series door ajar sounders
k. Tripp-Lite Model# IBAR4 or an approved equivalent surge suppressor
l. Handicapped door opener interfaces
m. Altronix AL400ULACMCB or equivalent power supply
n. Von Duprin EPT-10 power transfer device

2.5 TYCO SOFTWARE HOUSE iSTAR (ADVANCED PROCESSING CONTROLLER)

A. iSTAR Advanced Processing Controller Description: The iSTAR specified herein shall be used to control the locking/unlocking of doors.

B. iSTAR Feature/Capability Summary: The following indicates the iSTAR capabilities, capacities, and formats:

1. Advanced Processing Controller (iSTAR): The iSTAR shall include the following features:

a. Must have re-programmable FLASH memory for software upgrades and future product enhancements.
b. Must contain a 3,000 Event history buffer (minimum)

c. Must support 50,000 or greater card holders
d. Possess the capability of 255 time commands for automatic input, output, and reader mode control
e. Must have the ability of elevator control
f. Must possess real-time full-year clock and calendar
g. Must retain up to 80 hours of memory retention in the event of extended power failure

2. Inputs and Outputs: The Inputs and Outputs shall include the following features:

a. Thirty-two supervised and programmable inputs
b. Sixteen programmable Form C SPDT dry contacts rated at 2.5 amps @ 30V AC/DC outputs for reader controlled unlocking of doors

C. iSTAR System Interface Requirements

1. Grounding: Properly ground the iSTAR panel to prevent electrostatic charges and other transient electrical surges from damaging the panel.
2. Primary power: Connect the iSTAR panel to a dedicated 120 VAC power source through the external power supply.
3. Power supervision: The external power supply shall provide contacts that activate when there is an AC power failure and the system will report a "Power Failure" message to the CCure server.
4. Communications: Connect the iSTAR to the MSS485 terminal server for communications and programming with the CCure host server.
5. Housing: Install the iSTAR in a 16 AWG metal wall mounted lockable cabinet with tamper switches on the front and rear. (Standard Software House Cabinet).

2.6 HID GLOBAL SIGNO 20 CARD READER [CR]

A. Signo 20 Card Reader Description: The card reader specified herein shall be used to read Pennsylvania State University smart cards for the purpose of providing access control to secured areas of the University Park campus.

1. Signo 20 Feature/Capability Summary: The following indicates reader capabilities and formats:

a. 13.56 MHz (NFC) credentials via MIFARE DESFire EV1/EV2
b. Typical read range for MIFARE DESFire EV1/EV2: 1.6 to 4 inches.
c. Mounting: Mullion-mount door installation or any flat surface.
d. Color: Black bezel with silver trim baseplate.
e. Dimensions: 1.77 inches by 4.78 inches by 0.77 inches.
f. Operating Voltage: 12 volts DC.
g. Environmental Rating: UL294 Outdoor and Indoor rated, IP65.
h. Transmit Frequency: 125 kHz, 12.56 MHz (NFC), 2.4 GHz (Bluetooth).
i. Certifications (US): UL294/cUL, FCC.
j. Housing: Polycarbonate, UL94 V0.
k. Warranty: Limited Lifetime.

2.7 ALTRONIX MAXIM3D POWER SUPPLY [DPS]

A. Altronix Power Supply Description: The MAXIM3D distributes and routes power to access control systems and accessories. It will convert an 115VAC 50/60Hz input into eight (8) independently controlled PTC protected class 2 power limited 12VDC or 24VDC outputs. Outputs are activated by an open collector sink or normally open (NO) dry trigger input from an Access Control System, Card Reader, Keypad, Push Button, PIR, etc.

The unit will route power to a variety of access control hardware devices including: Magnetic Locks, Electric Strikes, Magnetic Door Holders, etc. Outputs will operate in both fail-safe and/or fail-secure modes.

The FACP Interface enables Emergency Egress, Alarm Monitoring, or may be used to trigger other auxiliary devices. The fire alarm disconnect function can be configured for the following modes: a) eight (8) outputs affected or b) four (4) outputs affected and four (4) outputs unaffected (50/50 mode).

B. Altronix Power Supply Features/Capability Summary:

1. 4 amp continuous supply current at 12 VDC or 24 VDC.
2. Eight (8) Access Control System trigger inputs.
3. Fire Alarm disconnect.
4. Automatic switchover to stand-by battery when AC fails.
5. Thermal and short-circuit protection with auto reset.
6. Battery failure and battery presence supervision.
7. AC failure supervision.

C. Altronix Power Supply Interface Requirements:

1. Primary Power: Connect the power supply to a non-switched, dedicated 120 VAC power source.
2. Power Supervision: Connect the power supply's supervisory outputs to the iSTAR panel.
3. Battery Back-up: Provide for a minimum 12 hours of back-up power in the event of primary power failure.

2.8 CABLES

A. General Cable Requirements: Comply with requirements in Section 26 05 19 "Low-Voltage Electrical Power Conductors and Cables" and as recommended by system manufacturer for integration requirement.

B. Paired, Plenum-Type, Reader and Wiegand Keypad Cables:

1. Three pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, individual aluminum-foil/polypropylene-tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and fluorinated-ethylene-propylene jacket, white color.
2. NFPA 70, Type CMP.
3. Flame Resistance: NFPA 262 flame test.

C. Multiconductor, Plenum-Type, Reader and Wiegand Keypad Cables:

1. Six conductors, No. 20 AWG, stranded (7x28) tinned copper conductors, fluorinated-ethylene-propylene insulation, overall aluminum-foil/polyester-tape shield with 100 percent shield coverage plus tinned copper braid shield with 85 percent shield coverage, and fluorinated-ethylene-propylene jacket, white color.
2. NFPA 70, Type CMP.
3. Flame Resistance: NFPA 262 flame test.

D. LAN Cabling:

1. Comply with requirements in Section 27 15 13 "Communications Copper Horizontal Cabling."

2.9 TRANSFORMERS

A. NFPA 70, Class II control transformers, NRTL listed. Transformers for security access-control system shall not be shared with any other system.

PART 3 - EXECUTION

3.1 BUILDING SECURITY

A. Building security shall remain functional during installation. Doors and door locking shall remain operational. University Police must be notified if it is not possible to lock the doors at the end of each workday. Failure to comply will result in removal from the approved vendor list.

3.2 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

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

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

3.3 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with TIA 606-B, "Administration Standard for Commercial Telecommunications Infrastructure."

C. Product Schedules: Obtain detailed product schedules from manufacturer of access-control system or develop product schedules to suit Project. Fill in all data available from Project plans and specifications and publish as Product Schedules for review and approval.

D. In meetings with Architect and Owner, present Product Schedules and review, adjust, and prepare final setup documents. Use approved, final Product Schedules to set up system software.

3.4 CABLING

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

B. Install cables and wiring according to requirements in Section 26 05 19 "Low-Voltage Electrical Power Conductors and Cables."

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

D. Firestopping: All cables penetrating floors and fire-rated walls must be routed through a properly firestopped metallic sleeve or a rated firestopping device to maintain the fire rating of the floor or wall.

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

F. Boxes and enclosures containing security-system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

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

3.5 CABLE APPLICATION

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

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

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

D. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from controller to the reader is 250 ft., and install No. 20 AWG wire if maximum distance is 500 ft..
3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the controller.

4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

E. Install minimum No. 16 AWG cable from controller to electrically powered locks. Do not exceed 250 ft. between terminations.

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

3.6 GROUNDING

A. Comply with Section 27 05 26 "Grounding and Bonding for Communications Systems."

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

C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

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

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.

3.7 INSTALLATION

A. Install card readers, keypads, push buttons, and biometric readers.

3.8 IDENTIFICATION

A. In addition to requirements in this article, comply with applicable requirements in Section 27 05 53 "Identification for Communications Systems" and with TIA 606-B.

B. Using software specified in "Cable and Asset Management Software" Article, 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 the same designation. Use logical and systematic designations for facility's architectural arrangement, as well as the University's standard naming conventions.

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.

3.9 SYSTEM SOFTWARE AND HARDWARE

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

B. Complete the programming of all inputs, outputs, readers, events, doors, and control panels. Programming of the system shall include the following:

1. Programming system configuration parameters (hardware and software, door location/number, communication parameters)
2. Programming operational parameters such as unlocking/locking times, events, door shunt times, and communication failure/restore times.
3. Other programming tasks required by Owner. Coordinate these additional programming requirements directly with the Owner.

3.10 FIELD QUALITY CONTROL

A. Field Coordination: Prior to installation, coordinate installation work with Architect, General Contractor, Electrical Contractor, Door/Hardware Contractor, and any other contractors associated with the system.

B. Acceptance Test Plan Form: Provide an Acceptance Test Plan Form to the Owner prior to performing an acceptance walk through. Include on the form separate sections for each device, panel, and unit, as well as a column indicating the manufacturer's performance allowance/margin, a column indicating the result of the testing performed by the Contractor (pass/fail), and an empty column for recording findings during the walk through.

C. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.
2. Certify completion in writing and schedule a commissioning walk-through. Provide all tools and personnel needed to conduct an efficient commissioning process.

D. Tests and Inspections:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use tester approved for type and kind of installed cable. Test for faulty connectors, splices, and terminations. Test according to TIA 568-C.1, "Commercial Building Telecommunications Cabling Standards - Part 1: General Requirements." Link performance for balanced twisted-pair cables must comply with minimum criteria in TIA 568-C.1.

2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power-supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

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

F. Prepare test and inspection reports. Provide a hard copy system printout of all components tested. Certify 100 percent operation indicating all devices, panels, units, and other components have passed the test criteria set forth by the manufacturer.

G. Maintain updated drawings at the site and markup any changes to the location of devices or routing of cabling caused by field conditions, bulletins, or as otherwise directed by the Architect. At the completion of the project, provide a final set of markup drawings to the Architect for the creation of "as-built" drawings.

3.11 STARTUP SERVICE

A. Engage a factory-authorized service representative to supervise and assist with startup service.

1. Complete installation and startup checks according to approved procedures that were developed in "Preparation" Article and with manufacturer's written instructions.
2. Enroll and prepare badges and access cards for Owner's operators, management, and security personnel.

3.12 DEMONSTRATION

A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain security access system. See Section 01 79 00 "Demonstration and Training."

B. Provide up to three (3) hours of on-site training, including:

1. Training on the proper installation and programming of all related hardware and software.
2. Training of departmental end-users.

C. Develop separate training modules for the following:

1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software.
2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel.
3. Security personnel.
4. Hardware maintenance personnel.
5. Campus management.

3.13 WARRANTY SERVICE

A. Contractor shall be responsible for maintenance and repair of the system during the warranty period, free of charge (parts and labor), including repair of defects in workmanship.

B. Contractor shall correct any system defect within six (6) hours of receipt of call from Owner.

C. Contractor shall offer extended service/maintenance agreements up to four (4) years after the warranty expires. The agreement shall be renewable monthly, quarterly, or yearly.

END OF SECTION