# SECTION 281300 - ACCESS CONTROL

Last Update: 9.26.14 File reformatted.

(Engineer shall edit specifications and blue text in header to meet project requirements. This includes but is not limited to updating Equipment and/or Material Model Numbers indicated in the specifications and adding any additional specifications that may be required by the project. Also turn off all "Underlines".)

## 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 and all other sections of Division 28.

### 1.2 SUMMARY

A. Section Includes:

1. Security access central-control station.
2. One or more security access networked workstations.
3. Security access operating system and application software.
4. Security access controllers connected to high-speed electronic-data transmission network.

B. Work includes, but is not limited to the following:

1. Install and integrate Access Control, Alarm Monitoring, CCTV, Intercom, and related security hardware.
2. Configure local access panels in various closets and the Server's computer system to communicate with one another.
3. Enter security system databases hardware configuration.
4. Test security system communication and operation in accordance with the specification.
5. Train operators and the system managers.

C. Bidding Requirements:

1. Submit complete detailed proposals with line item cost representation for components and associated installation labor. Lump sum bids will not be accepted.
2. Include as part of the bid response the following items:

    a. Installation schedule with proposed manpower assignments,
    b. Resumes for project manager and lead engineer for this project.

3. Review associated "E" and "TA" Series electrical, low voltage infrastructure drawings to verify that necessary conduit and floor boxes will be provided by others. The Owner will provide no additional infrastructure to support the Access Control Systems. Any discrepancies with the identified infrastructure to support these systems should be questioned in the form of a request for information (RFI) during the bidding process. Be responsible for any additional infrastructure requirements after receipt of contract for this project.
4. Unspecified Equipment and Material: Any item of equipment or material not specifically addressed on the drawings or in this document and required to provide complete and functional Access Control Systems and Video Surveillance Systems shall be provided in a level of quality consistent with other specified items.

## 1.3 DEFINITIONS

A. CCTV: Closed-circuit television.

B. CPU: Central processing unit.

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

D. dpi: Dots per inch.

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

F. GFI: Ground fault interrupter.

G. 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.

H. I/O: Input/output.

I. LAN: Local area network.

J. 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.

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

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

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

N. PIB: Photo-Identification and Badging System.

O. RAS: Remote access services.

P. RF: Radio frequency.

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

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

S. 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.

T. UPS: Uninterruptible power supply.

U. USB: Universal serial bus.

V. WAN: Wide area network.

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

X. WMP: Windows media player.

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

Z. Windows: Operating system by Microsoft Corporation.

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

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

## 1.4 SUBMITTALS

A. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a

location on Drawings. Test and evaluation data presented in Product Data shall comply with SIA BIO-01.

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

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

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

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

C. Samples: For workstation outlets, jacks, jack assemblies, and faceplates. For each exposed product and for each color and texture specified.

D. Other Action Submittals:

1. Project planning documents as specified in Part 3 "Preparation".

E. Field quality-control reports.

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

1. Microsoft Windows software documentation.
2. PC installation and operating documentation, manuals, and software for the PC and all installed peripherals. Software shall include system restore, emergency boot diskettes, and drivers for all installed hardware. Provide separately for each PC.
3. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM of the hard-copy submittal.
4. System installation and setup guides with data forms to plan and record options and setup decisions.

G. Manuals: Final copies of the manuals shall be delivered within fourteen (14) days after completing the installation test. Each manual’s contents shall be identified on the cover.

The manual shall include names, addresses, and telephone numbers of the contractor responsible for the installation and maintenance of the system and the factory representatives for each item of equipment for each system. The manuals shall have a table of contents and labeled sections. The final copies delivered after completion of the installation test shall include all modifications made during installation, checkout, and acceptance testing. The manuals shall consist of the following available from the manufacturer:

1. Functional Design Manual: The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included.
2. Hardware Manual: The manual shall describe all equipment furnished including:

    a. General description and specifications
    b. Installation and check out procedures
    c. Equipment layout and electrical schematics to the component level
    d. System layout drawings and schematics
    e. Alignment and calibration procedures
    f. Manufacturers repair parts list indicating sources of supply

3. Software Manual: The software manual shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:

    a. Definition of terms and functions
    b. System use and application software
    c. Initialization, start up, and shut down
    d. Reports generation
    e. Details on forms customization and field parameters

4. Operators Manual: The operators manual shall fully explain all procedures and instructions for the operation of the system including:

    a. Computers and peripherals
    b. System start up and shut down procedures
    c. Use of system, command, and applications software
    d. Recovery and restart procedures
    e. Graphic alarm presentation
    f. Use of report generator and generation of reports
    g. Data entry
    h. Operator commands
    i. Alarm messages and reprinting formats
    j. System permissions functions and requirements

5. Maintenance Manual: The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.
6. Manuals shall be delivered on CD/DVD in an organized fashion based on manufacturer and product.

H. As-Built Drawings: During system installation, maintain a separate hard copy set of drawings, elementary diagrams, and wiring diagrams of the SMS to be used for record drawings. This set shall be accurately kept up to date by the Contractor with all changes and additions to the SMS. Copies of the final as-built drawings shall be provided to the end user in DXF format.

## 1.5 QUALITY ASSURANCE

A. Installing company must be on a pre-approved list furnished by the owner for installation services for this project.

B. Providers of manufactured components, installation, wiring and testing shall be the responsibility of a single contractor who is an authorized dealer for the product supplied and who has been continuously in business for a period of not less than five (5) years and is licensed as required by the jurisdictions where the work will occur to perform the work specified. The security contractor shall meet the following performance requirements:

C. Authorized Lenel dealer: The security firm shall be a Lenel dealer in good standing.

D. Technician Certification:

1. Technical personnel shall be certified by the factory for the installation and service of all Lenel components.

E. Security License Requirements: The security contractor and "all" personnel at the company (including technical and administrative staff) shall be licensed by the State of Maryland for a security license with the appropriate background checks. All employees will have a formal background check and go through a drug-testing program during their initial hire in your firm as a standard procedure.

F. Service Support: Provide post-sales service support for all components in the system design that meets these requirements:

G. Availability: Seven (7) days a week, twenty four (24) hours a day.

H. Response Time: Two (2) hours to four (4) hours on-site.

I. Advance Replacement:

1. Contractor shall provide advance replacements for any component, during periods of repair or maintenance, whenever it is required.
2. The contractor shall be able to provide advance loaners.

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

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

K. Source Limitations: Obtain central station, workstations, controllers, Identifier readers, and all software through one source from single manufacturer.

L. 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.

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

N. Comply with FCC - Part 15, "Radio Frequency Devices".

O. Comply with FCC - Part 68, "Communication of Terminal Equipment to the Telephone Network".

P. Comply with UL 294, "Access Control System Units".

Q. Comply with UL 1076, "Proprietary Burglar Alarm Unit and Systems".

R. Comply with IEEE, "Institute of Electrical and Electronics Engineers".

S. Comply with Microsoft® Open Database Connectivity (ODBC) interface.

T. Comply with ISO Software Coding Standards for C++ and C##.

U. Comply with RoHS, "Restriction of Hazardous Substances".

V. Comply with [SIA DC-01 and ] SIA DC-03[ and SIA DC-07]. <Engineer to Edit for Project Requirements>

## 1.6 SYSTEM DESCRIPTION

A. Complete Engineering, installation, programming and maintenance of the security system for the [Insert Project/Building Name]. This system will consist of two (2) subsystems: access control (Lenel), Intercom (Aiphone and Code Blue systems).

## 1.7 CONTRACTOR PERFORMANCE REQUIREMENTS

A. Technical Personnel: The contractor shall have adequate technical staff located within thirty (30) miles of the university. At minimum, the contractor shall have at least twenty five (25) employees that are locally based in the Baltimore-Washington corridor.

B. Working Hours Response: During normal working hours, all telephone calls placed to the contractor shall be answered by a live person, not an auto-attendant.

C. Service Dispatch: The contractor shall use a computerized service dispatch system that is a commercial off-the-shelf product used for dispatching service companies. At the end of every week, the contractor will be required to email the hospital a list of all service calls and their status on an automatic basis. Excel spreadsheets are not acceptable for a service dispatch program.

D. The contractor shall have a dedicated position specifically for managing and dispatching service calls for their clients. This position shall perform no other functions except service-related dispatch functions and services.

E. Engineering: The contractor must have field-trained engineers on staff that are 100% conversant in AutoCAD and are able to provide the necessary electronic drawings and submittals required for a project of this size. The engineer must also be certified at the Master level in Lenel.

F. Contractor must meet all security clearance requirements to meet NBHPP CHEMPAK standards

G. The contractor must be a certified dealer of all products utilized in the system to include: Lenel, American Dynamics, Aiphone, Code Blue, HID, Pelco

1.8 SUBSTITUTIONS AND QUALITY:

A. Where products are specified by name, provide and install that product. Substitutions will not be accepted for the access control or digital CCTV system or their sub-systems.

1.9 DELIVERY, STORAGE, AND HANDLING

A. Environmental Limitations: Do not deliver or install cables and connecting materials until wet work in spaces is complete and dry, and temporary HVAC system is operating and maintaining ambient temperature and humidity conditions at occupancy levels during the remainder of the construction period.

B. Environmental Limitations: Do not deliver or install equipment until spaces are enclosed and weather tight, wet work in spaces is complete and dry, and work above ceilings is complete.

C. Central Station, Workstations, and Controllers:

1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50$^0$F and 85$^0$F, and not more than 80 percent relative humidity, noncondensing.
2. Open each container; verify contents against packing list; and file copy of packing list, complete with container identification, for inclusion in operation and maintenance data.
3. Mark packing list with the same designations assigned to materials and equipment for recording in the system labeling schedules that are generated by software specified in "Cable and Asset Management Software" Article.
4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

## 1.10 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$^0$F to 85$^0$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$^0$F to 122$^0$F dry bulb and 20 to 90 percent relative humidity, noncondensing.
3. Indoor, Uncontrolled Environment: NEMA 250, Type 12 enclosures. System components installed in non-temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of 0$^0$F to 122$^0$F dry bulb and 20 % to 90 % relative humidity, noncondensing.
4. 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$^0$F to plus 122$^0$F dry bulb and 20 % to 90 % relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to eighty five (85) mph and snow cover up to twenty four (24) inches thick.
5. Hazardous Environment: System components located in areas where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers shall be rated, listed, and installed according to NFPA 70.
6. Corrosive Environment: For system components subjected to corrosive fumes, vapors, and wind-driven salt spray in coastal zones, provide NEMA 250, Type 4X enclosures.

## 1.11 EXTRA MATERIALS

A. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Alarm Printer Black/Red Ribbons: Package of 12.
2. Laser Printers: Three toner cassettes and one replacement drum unit.
3. Credential card blanks, ready for printing. Include 1,000 credential cards.
4. Fuses of all kinds, power and electronic, equal to 10 percent of amount installed for each size used, but no fewer than three units.

## 1.12 SERVICE AND MAINTENANCE

A. Owner's security personnel in operation and management operations, including changing signal pathways for different workstations, rerouting signals in failed cables, and keeping records of access assignments and revisions when extending elements to establish new access outlets.

B. General Requirements: Provide all services required and equipment necessary to maintain the entire SMS in an operational state as specified for a period of two (2) year(s) after formal written acceptance of the system, and shall provide all necessary material required for performing scheduled service or other unscheduled work.

C. Description of Work: The service and repair of the SMS including all equipment provided under this specification supplied by the successful contractor. Provide the manufacturer's required scheduled and unscheduled maintenance and all other work necessary to keep the SMS at its maximum performance.

D. Personnel: Service personnel shall be factory certified in the maintenance and repair of the equipment installed under this section of the specification. The owner shall be advised in writing of the name of the designated service representative, and of any change in personnel.

E. Schedule of Work: This work shall be performed during regular working hours (8-5), Monday through Friday, excluding federal holidays.

1. Inspections: The Contractor shall perform two minor inspections at 6 month intervals (or more often if required by the manufacturer), and two major inspections offset equally between the minor inspections to effect quarterly inspection of alternating magnitude.
2. Minor Inspections: These inspections shall include:

a. Visual checks and operational tests of all console equipment, peripheral equipment, field hardware, sensors, and electrical and mechanical controls.

b. Mechanical adjustments if required on any mechanical or electromechanical devices

3. Major Inspections: These inspections shall include all work described under paragraph Minor Inspections and the following work:

a. Clean all SMS equipment, including interior and exterior surfaces.
b. Perform diagnostics on all equipment.
c. Check, walk test, and if required by the manufacturer's maintenance procedures, calibrate each sensor.
d. Run all system software diagnostics and correct all diagnosed problems.

F. Operation: Performance of scheduled adjustments and repair shall verify operation of the SMS as demonstrated by the applicable tests of the performance verification test.

G. Emergency Service: The owner will initiate service calls when the SMS is not functioning properly and hinders critical operation of the facility. Qualified personnel shall be available to provide service to the complete SMS repairs. The owner shall be furnished with a telephone number where the service supervisor can be reached at all times. Service personnel shall be at site within four (4) hours after receiving a request for service. The SMS shall be restored to proper operating condition within eight (8) hours after service personnel arrive on site.

H. Records and Logs: Keep records and logs of each task, and shall organize cumulative records for each component, and for the complete system chronologically. A continuous log shall be maintained for all devices. The log shall contain all initial settings. Complete logs shall be kept and shall be available for inspection on site, demonstrating that planned and systematic adjustments and repairs have been accomplished for the SMS.

I. Work Requests: Separately record each service call request on a service request form. The form shall include the model and serial number identifying the component involved, its location, date and time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing what has to be done, the amount and nature of the materials used, the time and date work started, and the time and date of completion. Deliver a record of the work performed within 5 days after work is accomplished.

J. System Modifications: Make any recommendations for system modification in writing to the Owner. No system modifications shall be made without prior approval of the Owner. Any modifications made to the system shall be incorporated into the operations and maintenance manuals, and other documentation affected.

K. Software: Provide all software updates during the period of the warranty and verify operation in the system. These updates shall be accomplished in a timely manner, fully coordinated with SMS operators, shall include training for the new changes/features

enabled, and shall be incorporated into the operations and maintenance manuals, and software documentation.

## 1.13 COMMISSIONING AND STARTUP

A. Program all newly installed field hardware into the existing system. All controllers, door interfaces, input and output panels should be entered and configured per operational guidelines provided by the hospital.

B. Follow all applicable business rules utilized in the existing system.

C. Supply training for personnel for data entry of cardholder information, badge printing and access level assignments. Contractor is not responsible for cardholder creation or badge production.

## 1.14 WARRANTY/GUARANTEE

A. See Division 26 Specification Section "Basic Electrical Requirements' for warranty and guarantee requirements.

B. During the first year, provide a full service warranty program that guarantees a two (2) hours to four (4) hours on site response, include all parts and labor, and provides advance replacements for any defective components. The installation contractor must qualify as the service organization and provide the on-site warranty service.

C. The system components shall be guaranteed against all defective materials, design and workmanship for a period of two (2) years from the date of acceptance by the client after final testing. New replacement parts shall be furnished promptly and defects in design and workmanship shall be corrected, without cost to the Owner, promptly upon receipt of notice from the Owner of failure of any part of the system during the guarantee period. This is a one year full parts and labor warranty and no alternative will be acceptable.

D. Any item failing before the one (1) year guarantee period expires shall be replaced and the guarantee extended for that item for twelve (12) months from the replacement date of the item.

E. The warranty period for any part which has a warranty by the manufacturer of longer than twelve (12) months shall be for the longer period. Provide a copy of the manufacturer's warranty period statement for all alarm equipment, all software, all major components, and other major devices.

## PART 2 - PRODUCTS

### 2.1 DESCRIPTION

A. Security Access System: PC-based central station, one or more networked PC-based workstations, and field-installed controllers, connected by a high-speed electronic-data transmission network.

B. System Software: Based on thirty two (32) bit, Windows 2,000 central-station, workstation operating system, server operating system, and application software. Software shall have the following capabilities:

1. Multiuser and multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
2. Graphical user interface to show pull-down menus and a menu-tree format that complies with interface guidelines of Microsoft Windows.
3. System license for the entire system including capability for future additions that are within the indicated system size limits specified in this Section.
4. Open-architecture system that allows importing and exporting of data and interfacing with other systems that are compatible with Microsoft Windows and shall be written to Microsoft's published standards for User Interface Design, Secure Coding Practices and Database Implementation Guidelines (Microsoft® Open Database Connectivity (ODBC) interface).
5. Password-protected operator login and access.
6. Open-database-connectivity compliant.

C. The SMS shall utilize an open architecture where all data must reside on a single database and must be accessible in real time to every / any SMS workstation or web based client connected to the network. The system shall be configurable to support all of the following databases: Microsoft SQL Server 2,000 – Personal and Standard editions with SP3a, Microsoft SQL Server 2005 – Standard and Enterprise editions and Microsoft SQL Server 2005 Express, Oracle Server 9.i. and Oracle Server 10g. Oracle data may reside on Windows or UNIX platforms.

D. The system architecture shall support Microsoft Windows Clustering, Hot-Standby, Fault Tolerant Servers and Fault Tolerant Hot Standby Servers.

E. The SMS shall be able to connect to and interface bi-directionally with external data sources utilizing all of the following methods:

1. ASCII with support for XML formatted text exchange of data activated both manually and automatically.
2. ASCII with support for XML formatted text exchange of data using a direct table interface activated both manually and automatically.

3. Real-time exchange of data via Active Directory/LDAP utilizing an API written by the SMS manufacturer. The live exchange of data shall expose SMS events and transactions to other data sources in real-time and allow for receipt of data into the SMS where this data may be acted upon and trigger linked events in the SMS in real-time.
4. Real-time exchange of information utilizing a IBM WebSphere adapter.

F. The SMS shall support

1. Lenel OnGuard® PRO Series with Unlimited number of Access Control Readers, Unlimited number of Inputs/Outputs, Unlimited number of Client Workstations, Unlimited number of Cardholders

G. Network connecting the central station and workstations shall be a [LAN] [WAN] <Insert type> using Microsoft Windows-based TCP/IP with a capacity of connecting up to 99 workstations. System shall be portable across multiple communication platforms without changing system software.

H. Network(s) connecting PCs and controllers shall consist of one or more of the following:

1. Local area, IEEE 802.3 Fast Ethernet Gigabit-Ethernet, star topology network based on TCP/IP.
2. Direct-connected, RS-232 cable from the COM port of the central station to the first controller, then RS-485 cable to interconnect the remaining controllers at that Location.
3. Dial-up and cable modem connection using a standard cable or dial-up telephone line.

## 2.2 OPERATION

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

B. Distributed Processing: A fully distributed processing system.

1. Access-control information, including time, date, valid codes, access levels, and similar data, shall be downloaded to controllers so each controller can make access-control decisions.
2. Intermediate controllers for access control are prohibited.
3. In the event that communications with the central controller are lost, controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the central station.

C. Number of Locations:

1. Support at least thirty two thousand (32,000) separate Locations using a single PC with combinations of direct-connect, dial-up, or TCP/IP LAN connections to each Location.
2. Each Location shall have its own database and history in the central station.
3. Locations may be combined to share a common database.

D. Data Capacity:

1. [One hundred thirty (130)] <Insert number> different card-reader formats.
2. [Nine hundred ninety nine (999)] <Insert number> comments.
3. [Forty eight (48)] <Insert number> graphic file types for importing maps.

E. Location Capacity:

1. Five hundred twelve (512) reader-controlled doors, scalable to one thousand (1,000) in future.
2. [Fifty thousand (50,000)] <Insert number> total-access credentials.
3. Five hundred (500) supervised alarm inputs, scalable to one thousand (1,000) in future.
4. [Two thousand forty eight (2,048)] <Insert number> programmable outputs.
5. [Thirty two thousand (32,000)] <Insert number> custom action messages per Location to instruct operator on action required when alarm is received.

F. System Network Requirements:

1. System components shall be interconnected and shall provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
2. Communication shall not require operator initiation or response and shall return to normal after partial- or total-network interruption such as power loss or transient upset.
3. System shall automatically annunciate communication failures to the operator and shall identify the communications link that has experienced a partial or total failure.
4. Communications controller may be used as an interface between the central-station display systems and the field device network. Communications controller shall provide functions required to attain the specified network communications performance.

G. Central station shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central station shall control system networks to interconnect all system components, including workstations and field-installed controllers.

H. Field equipment shall include controllers, sensors, and controls.

1. Controllers shall serve as an interface between the central station and sensors and controls.
2. Data exchange between the central station and the controllers shall include down-line transmission of commands, software, and databases to controllers.
3. The up-line data exchange from the controller to the central station shall include status data such as intrusion alarms, status reports, and entry-control records.
4. Controllers are classified as alarm-annunciation or entry-control type.

I. System Response to Alarms:

1. Field device network shall provide a system end-to-end response time of one second(s) or less for every device connected to the system.
2. Alarms shall be annunciated at the central station within one second of the alarm occurring at a controller or at a device controlled by a local controller, and within one hundred (100) ms if the alarm occurs at the central station.
3. Alarm and status changes shall be displayed within 100 ms after receipt of data by the central station.
4. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within five seconds of alarm receipt at the security console.
5. This response time shall be maintained during system heavy load.

J. False-Alarm Reduction: The design of the central station and controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

K. Error Detection:

1. Use a cyclic code method to detect single- and double-bit errors, burst errors of eight bits or fewer, and at least 99 % of all other multibit and burst errors between controllers and the central station.
2. Interactive or product error-detection codes alone will not be acceptable.
3. A message shall be in error if one (1) bit is received incorrectly.
4. Retransmit messages with detected errors.
5. Allow for an operator-assigned two (2) digit decimal number to each communications link representing the number of retransmission attempts.
6. Central station shall print a communication failure alarm message when the number of consecutive retransmission attempts equals the assigned quantity.
7. Monitor the frequency of data transmission failure for display and logging.

L. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

M. Door Hardware Interface:

1. Comply with requirements in Division 08 Sections for door hardware required to be monitored or controlled by the security access system.

2. Electrical characteristics of controllers shall match the signal and power requirements of door hardware.

## 2.3 APPLICATION SOFTWARE

A. System Software: Based on [thirty two (32)] <Insert number>-bit, Microsoft Windows 2,000 central-station and workstation operating system and application software.

1. Multiuser multitasking shall allow independent activities and monitoring to occur simultaneously at eight (8) different workstations, expandable to sixteen (16).
2. Graphical user interface shall show pull-down menus and a menu-tree format.
3. Capability for future additions within the indicated system size limits.
4. Open architecture that allows importing and exporting of data and interfacing with other systems including Photo-ID and Badging (PIB) systems and other sytems that are compatible with operating system.
5. Password-protected operator login and access.

B. Peer Computer Control Software: Detect a failure of a central computer and cause the other central computer to assume control of all system functions without interruption of operation. Both central computers shall have drivers to support this mode of operation.

C. Application Software: Interface between the alarm annunciation and entry-control controllers to monitor sensors[ and DTS links], operate displays, report alarms, generate reports, and help train system operators. <Engineer to Edit for Project Requirements>

1. Reside at the central station, workstations, and controllers as required to perform specified functions.
2. Operate and manage peripheral devices.
3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.
4. Import custom icons into graphics to represent alarms and I/O devices.
5. Globally link I/O so that any I/O can link to any other I/O within the same Location without requiring interaction with the host PC. This operation shall be at the controller.
6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the controller.
7. Messages from PC to controllers and controllers to controllers shall be on a polled network that utilizes check summing and acknowledgment of each message. Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.
8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-controller communications

methods by changing the polling frequency and the amount of time the system waits for a response.

9. Automatic and encrypted backups for database and history backups shall be automatically stored at the central-control PC and encrypted with a nine-character alphanumeric password that must be used to restore or read data contained in backup.
10. Operator audit trail for recording and reporting all changes made to database and system software.
11. Support network protocol and topology, TCP/IP, Novel Netware, Digital Pathworks, Banyan Vines, LAN/WAN, and RAS.

D. Workstation Software:

1. Password levels shall be individually customized at each workstation to allow or disallow operator access to program functions for each Location.
2. Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation. If an alarm is unacknowledged (not handled by another workstation) for a preset amount of time, the alarm will automatically appear on the filtered workstation.

E. Controller Software:

1. Controllers shall operate as autonomous, intelligent processing units.

    a. Controllers shall make decisions about access control, alarm monitoring, linking functions, and door-locking schedules for their operation, independent of other system components.
    b. Controllers shall be part of a fully distributed processing-control network.
    c. The portion of the database associated with a controller, and consisting of parameters, constraints, and the latest value or status of points connected to that controller, shall be maintained in the controller.

2. The following functions shall be fully implemented and operational within each controller:

    a. Monitoring inputs.
    b. Controlling outputs.
    c. Automatically reporting alarms to the central station.
    d. Reporting of sensor and output status to the central station on request.
    e. Maintaining real time, automatically updated by the central station at least once a day.
    f. Communicating with the central station.
    g. Executing controller resident programs.
    h. Diagnosing.
    i. Downloading and uploading data to and from the central station.

3. Controller Operations at a Location:

   a. Up to sixteen (16) controllers connected to TIA 485-A communications loop. Globally operating I/O linking and anti-passback functions between controllers within the same Location without central-station or workstation intervention. Linking and anti-passback shall remain fully functional within the same Location even when the central station or workstations are off-line.
   b. In the event of communication failure between the central station and a Location, there shall be no degradation in operations at the controllers at that Location. Controllers at each Location shall be connected to a memory buffer with a capacity to store up to ten thousand (10,000) events; there shall be no loss of transactions in system history files until the buffer overflows.
   c. Buffered events shall be handled in a first-in-first-out mode of operation.

4. Individual Controller Operation:

   a. Controllers shall transmit alarms, status changes, and other data to the central station when communications circuits are operable. If communications are not available, controllers shall function in a stand-alone mode; operational data, including the status and alarm data normally transmitted to the central station, shall be stored for later transmission to the central station. Storage capacity for the latest one thousand twenty four (1,024) events shall be provided at each controller.
   b. Card-reader ports of a controller shall be custom configurable for at least [one hundred twenty (120)] <Insert number> different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different controllers or within the same controller.
   c. Controllers shall provide a response to card readers or keypad entries in less than 0.25 seconds, regardless of system size.
   d. Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to their proper working state. This shall happen without any operator intervention.
   e. Initial Startup: When controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each controller.
   f. On failure for any reason, controllers shall perform an orderly shutdown and force controller outputs to a predetermined failure-mode state, consistent with the failure modes shown and the associated control device.
   g. After power is restored, following a power failure, startup software shall initiate self-test diagnostic routines, after which controllers shall resume normal operation.
   h. After controller failure, if the database and application software are no longer resident, controllers shall not restart but shall remain in the failure

mode until repaired. If database and application programs are resident, controllers shall immediately resume operation. If not, software shall be restored automatically from the central station.

5. Communications Monitoring:

   a. System shall monitor and report status of TIA 485-A communications loop of each Location.
   b. Communication status window shall display which controllers are currently communicating, a total count of missed polls since midnight, and which controller last missed a poll.
   c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM for each controller.

6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the central station at least once a day to plus or minus 10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

F. PC-to-Controller Communications:

1. Central-station or workstation communications shall use the following:

   a. Direct connection using serial ports of the PC.
   b. TCP/IP LAN interface cards.
   c. Dial-up or cable modems for connections to Locations.

2. Each serial port used for communications shall be individually configurable for "direct communications," "modem communications incoming and outgoing," or "modem communications incoming only," or as an ASCII output port. Serial ports shall have adjustable data transmission rates and shall be selectable under program control.
3. Use multiport communications board if more than two serial ports are needed.

   a. Use a four (4), eight (8), or sixteen (16) serial port configuration that is expandable to thirty two (32) or sixty four (64) serial ports.
   b. Connect the first board to an internal PCI bus adapter card.

4. Direct serial, TCP/IP, and dial-up, cable, or satellite communications shall be alike in the monitoring or control of the system except for the connection that must first be made to a dial-up or voice-over IP Location.
5. TCP/IP network interface card (NIV) shall have an option to set the poll-frequency and message-response time-out settings.
6. PC-to-controller and controller-to-controller communications (direct, dial-up, or TCP/IP) shall use a polled-communication protocol that checks sum and

acknowledges each message. All communications in this subparagraph shall be verified and buffered, and retransmitted if not acknowledged.

G. Direct Serial or TCP/IP PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-controller communications link.
2. Loss of communications to any controller shall result in an alarm at all PCs running the communication software.
3. When communications are restored, all buffered events shall automatically upload to the PC, and any database changes shall be automatically sent to the controller.

H. Dial-up Modem or Cable Modem PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-controller communications link during dial-up modem connect times.
2. Communication software shall be programmable to routinely poll each of the remote dial-up or cable modem Locations, collecting event logs and verifying phone lines at operator-selectable time intervals for each Location.
3. System shall be programmable for dialing and connecting to all dial-up or cable modem Locations and for retrieving the accrued history transactions on an automatic basis as often as once every [ten (10)] <Insert number> minutes and up to once every [nine thousand nine hundred ninety nine (9,999)] <Insert number> minutes.
4. Failure to communicate to a dial-up Location three times in a row shall result in an alarm at the PC.
5. Time offset capabilities shall be present so that Locations in a different geographical time zone than the host PC will be set to, and maintained at, the proper local time. This feature shall allow for geographical time zones that are ahead of or behind the host PC.
6. The controller connected to a dial-up or cable modem shall automatically buffer all normal transactions until its buffer reaches 80 percent of capacity. When the transaction buffer reaches 80 %, the controller shall automatically initiate a call to the central station and upload all transactions.
7. Alarms shall be reported immediately.
8. Dial-up or cable modems shall be provided by manufacturer of the system. Modems used at the controller shall be powered by the controller. Power to the modem shall include battery backup if the controller is so equipped.

I. Controller-to-Controller Communications:

1. TIA 485-A, four-wire, point-to-point, regenerative (repeater) communications network methodology.
2. TIA 485-A communications signal shall be regenerated at each controller.

J. Database Downloads:

1. All data transmissions from PCs to a Location, and between controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a controller is reset for any reason, it shall automatically request and receive a database download from the PC. The download shall restore data stored at the controller to their normal working state and shall take place with no operator intervention.
3. Software shall provide for setting downloads via dial-up connection to once per twenty four (24) hour period, with time selected by the operator.
4. Software shall provide for setting delays of database downloads for dial-up connections. Delays change the download from immediately to a delay ranging from one to nine hundred ninety nine (999) minutes.

K. Operator Interface:

1. Inputs in system shall have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons shall automatically change to the proper icon to display the current system state in real time. Icons shall also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a time zone or a manual command.
3. Outputs in system shall have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points shall be constantly updated to show their current real-time condition without prompting by the operator.
5. The operator shall be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Graphic maps or drawings containing inputs, outputs, and override groups shall include the following:

    a. Database to import and store full-color maps or drawings and allow for input, output, and override group icons to be placed on maps.
    b. Maps to provide real-time display animation and allow for control of points assigned to them.
    c. System to allow inputs, outputs, and override groups to be placed on different maps.
    d. Software to allow changing the order or priority in which maps will be displayed.

7. Override Groups Containing I/Os:

a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
b. Icon shall change automatically to show the live summary status of points in that group.
c. Override group icon shall provide a method to manually control or set to time-zone points in the group.
d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.

8. Schedule Overrides of I/Os and Override Groups:

a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.
b. Each schedule shall be composed of a minimum of two dates with separate times for each date.
c. The first time and date shall be assigned the override state that the point shall advance to when the time and date become current.
d. The second time and date shall be assigned the state that the point shall return to when the time and date become current.

9. Copy command in database shall allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

L. Operator Access Control:

1. Control operator access to system controls through [three] <Insert number> password-protected operator levels. System operators and managers with appropriate password clearances shall be able to change operator levels for operators.
2. Three successive attempts by an operator to execute functions beyond their defined level during a twenty four (24) hour period shall initiate a software tamper alarm.
3. A minimum of [thirty two (32)] <Insert number> passwords shall be available with the system software. System shall display the operator's name or initials in the console's first field. System shall print the operator's name or initials, action, date, and time on the system printer at login and logoff.
4. The password shall not be displayed or printed.
5. Each password shall be definable and assignable for the following:

a. Selected commands to be usable.
b. Access to system software.
c. Access to application software.
d. Individual zones that are to be accessed.

e. Access to database.

M. Operator Commands:

1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.
2. Command inputs shall be acknowledged and processing shall start in not less than one second(s).
3. Tasks that are executed by operator's commands shall include the following:

a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.
b. Place Zone in Access: Used to remotely disable intrusion-alarm circuits emanating from a specific zone. System shall be structured so that console operator cannot disable tamper circuits.
c. Place Zone in Secure: Used to remotely activate intrusion-alarm circuits emanating from a specific zone.
d. System Test: Allows the operator to initiate a system-wide operational test.
e. Zone Test: Allows the operator to initiate an operational test for a specific zone.
f. Print reports.
g. Change Operator: Used for changing operators.
h. Security Lighting Controls: Allows the operator to remotely turn on or turn off security lights.
i. Display Graphics: Used to show any graphic displays implemented in the system. Graphic displays shall be completed within twenty (20) seconds from time of operator command.
j. Run system tests.
k. Generate and format reports.
l. Request help with the system operation.

1) Include in main menus.
2) Provide unique, descriptive, context-sensitive help for selections and functions with the press of one function key.
3) Provide navigation to specific topic from within the first help window.
4) Help shall be accessible outside the application program.

m. Entry-Control Commands:

1) Lock (secure) or unlock (open) each controlled entry and exit up to [four] <Insert number> times a day through time-zone programming.

2) Arm or disarm each monitored input up to [four (4)] <Insert number> times a day through time-zone programming.
3) Enable or disable readers or keypads up to [two (2)] <Insert number> times a day through time-zone programming.
4) Enable or disable cards or codes up to [four (4)] <Insert number> times a day per entry point through access-level programming.

4. Command Input Errors: Show operator input assistance when a command cannot be executed because of operator input errors. Assistance screen shall use plain-language words and phrases to explain why the command cannot be executed. Error responses that require an operator to look up a code in a manual or other document are not acceptable. Conditions causing operator assistance messages include the following:

a. Command entered is incorrect or incomplete.
b. Operator is restricted from using that command.
c. Command addresses a point that is disabled or out of service.
d. Command addresses a point that does not exist.
e. Command is outside the system's capacity.

N. Alarms:

1. System Setup:

a. Assign manual and automatic responses to incoming-point status change or alarms.
b. Automatically respond to input with a link to other inputs, outputs, or operator-response plans; unique sound with use of WAV files; and maps or images that graphically represent the point location.
c. Sixty-character message field for each alarm.
d. Operator-response-action messages shall allow message length of at least sixty five thousand (65,000) characters, with database storage capacity of up to thirty two thousand (32,000) messages. Setup shall assign messages to access point.
e. Secondary messages shall be assignable by the operator for printing to provide further information and shall be editable by the operator.
f. Allow twenty five (25) secondary messages with a field of four (4) lines of sixty (60) characters each.
g. Store the most recent one thousand (1,000) alarms for recall by the operator using the report generator.

2. Software Tamper:

a. Annunciate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful attempts to log onto system shall generate a software tamper alarm.

b. Annunciate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond the authorization level.
c. Maintain a transcript file of the last five thousand (5,000) commands entered at each central station to serve as an audit trail. System shall not allow write access to system transcript files by any person, regardless of their authorization level.
d. Allow only acknowledgment of software tamper alarms.

3. Read access to system transcript files shall be reserved for operators with the highest password authorization level available in system.
4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.
5. Multimedia Alarm Annunciation: WAV files to be associated with alarm events for audio annunciation or instructions.
6. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.
7. Alarm Automation Interface: High-level interface to central-station alarm automation software systems. Allows input alarms to be passed to and handled by automation systems in the same manner as burglar alarms, using a TIA 232-F ASCII interface.
8. CCTV Alarm Interface: Allow commands to be sent to CCTV systems during alarms (or input change of state) through serial ports.
9. Camera Control: Provides operator ability to select and control cameras from graphic maps.

O. Alarm Monitoring: Monitor sensors, controllers, and DTS circuits and notify operators of an alarm condition. Display higher-priority alarms first and, within alarm priorities, display the oldest unacknowledged alarm first. Operator acknowledgment of one alarm shall not be considered acknowledgment of other alarms nor shall it inhibit reporting of subsequent alarms.

1. Displayed alarm data shall include type of alarm, location of alarm, and secondary alarm messages.
2. Printed alarm data shall include type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator responses.
3. Maps shall automatically display the alarm condition for each input assigned to that map if that option is selected for that input location.
4. Alarms initiate a status of "pending" and require the following two handling steps by operators:

a. First Operator Step: "Acknowledged." This action shall silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."
b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm shall then clear.

5. Each workstation shall display the total pending alarms and total unresolved alarms.
6. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.
7. Alarms shall transmit to the central station in real time except for allowing connection time for dial-up locations.
8. Alarms shall be displayed and managed from a minimum of four different windows.

a. Input Status Window: Overlay status icon with a large red blinking icon. Selecting the icon will acknowledge the alarm.
b. History Log Transaction Window: Display name, time, and date in red text. Selecting red text will acknowledge the alarm.
c. Alarm Log Transaction Window: Display name, time, and date in red. Selecting red text will acknowledge the alarm.
d. Graphic Map Display: Display a steady colored icon representing each alarm input location. Change icon to flashing red when the alarm occurs. Change icon from flashing red to steady red when the alarm is acknowledged.

9. Once an alarm is acknowledged, the operator shall be prompted to enter comments about the nature of the alarm and actions taken. Operator's comments may be manually entered or selected from a programmed predefined list, or a combination of both.
10. For locations where there are regular alarm occurrences, provide programmed comments. Selecting that comment shall clear the alarm.
11. The time and name of the operator who acknowledged and resolved the alarm shall be recorded in the database.
12. Identical alarms from the same alarm point shall be acknowledged at the same time the operator acknowledges the first alarm. Identical alarms shall be resolved when the first alarm is resolved.
13. Alarm functions shall have priority over downloading, retrieving, and updating database from workstations and controllers.
14. When a reader-controlled output (relay) is opened, the corresponding alarm point shall be automatically bypassed.

P. Monitor Display: Display text and graphic maps that include zone status integrated into the display. Colors are used for the various components and current data. Colors shall be uniform throughout the system.

1. Color Code:

   a. "FLASHING RED": Alerts operator that a zone has gone into an alarm or that primary power has failed.
   b. "STEADY RED': Alerts operator that a zone is in alarm and alarm has been acknowledged.
   c. 'YELLOW": Advises operator that a zone is in access.
   d. "GREEN": Indicates that a zone is secure and that power is on.

2. Graphics:

   a. Support thirty two thousand (32,000) graphic display maps and allow import of maps from a minimum of sixteen (16) standard formats from another drawing or graphics program.
   b. Allow I/O to be placed on graphic maps by the drag-and-drop method.
   c. Operators shall be able to view the inputs, outputs, and the point's name by moving the mouse cursor over the point on the graphic map.
   d. Inputs or outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view graphic maps associated with I/Os.
   e. Each graphic map shall have a display-order sequence number associated with it to provide a predetermined order when toggled to different views.
   f. Camera icons shall have the ability to be placed on graphic maps that, when selected by an operator, will open a video window, display the camera associated with that icon, and provide pan-tilt-zoom control.
   g. Input, output, or camera placed on a map shall allow the ability to arm or bypass an input, open or secure an output, or control the pan-tilt-zoom function of the selected camera.

Q. System test software enables operators to initiate a test of the entire system or of a particular portion of the system.

   1. Test Report: The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.

R. Report-Generator Software: Include commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time. Report printing shall be the lowest-priority activity. Report-generation mode shall be operator selectable but set up initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.

   1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of the period; and the default printer.
   2. Printing on Request: An operator may request a printout of any report.

3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm (such as door alarm, intrusion alarm, tamper alarm, etc.), the type of sensor, the location, the time, and the action taken.
4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.
5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.
6. Automatic History Reports: Named, saved, and scheduled for automatic generation.
7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
10. Who Is "In" (Muster) Report:

    a. Emergency Muster Report: One-click operation on toolbar launches report.
    b. Cardholder Report. Contain a count of persons who are "In" at a selected Location and a detailed listing of name, date, and time of last use, sorted by the last reader used or by the group assignment.

11. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that data are available on-site at all times.
12. Activity and Alarm On-Line Printing: Activity printers for use at workstations; prints all events, or alarms only.
13. History Reports: Custom reports that allow the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.

    a. Initially store history on the hard disk of the host PC.
    b. Permit viewing of the history on workstations or print history to any system printer.
    c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.
    d. Each report shall depict the date, time, event type, event description, and device; or I/O name, cardholder group assignment, and cardholder name or code number.

e. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.
f. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total shall reflect how many alarms occurred during that period.

14. Reports shall have the following four options:

a. View on screen.
b. Print to system printer. Include automatic print spooling and "Print To" options if more than one printer is connected to the system.
c. "Save to File" with full path statement.
d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of time zone, manually overridden, not reporting, or in alarm.

15. Custom Code List Subroutine: Allow the access codes of system to be sorted and printed according to the following criteria:

a. Active, inactive, or future activate or deactivate.
b. Code number, name, or imprinted card number.
c. Group, Location access levels.
d. Start and stop code range.
e. Codes that have not been used since a selectable number of days.
f. In, out, or either status.
g. Codes with trace designation.

16. The reports of system database shall allow options so that every data field may be printed.
17. The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows.

S. Anti-Passback:

1. System shall have global and local anti-passback features, selectable by Location. System shall support hard and soft anti-passback.
2. Hard Anti-Passback: Once a credential holder is granted access through a reader with one type of designation (IN or OUT), the credential holder may not pass through that type of reader designation until the credential holder passes through a reader of opposite designation.
3. Soft Anti-Passback: Should a violation of the proper IN or OUT sequence occur, access shall be granted, but a unique alarm shall be transmitted to the control station, reporting the credential holder and the door involved in the violation. A separate report may be run on this event.

4. Timed Anti-Passback: A controller capability that prevents an access code from being used twice at the same device (door) within a user-defined amount of time.
5. Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at controller). Each reader shall be assignable to one or all four anti-passback zones. In addition, each anti-passback reader can be further designated as "Hard," "Soft," or "Timed" in each of the four anti-passback zones. The four anti-passback zones shall operate independently.
6. The anti-passback schemes shall be definable for each individual door.
7. The Master Access Level shall override anti-passback.
8. System shall have the ability to forgive (or reset) an individual credential holder or the entire credential-holder population anti-passback status to a neutral status.

T. Visitor Assignment:

1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only those access levels that have been designated as approved for visitors.
2. Provide an automated log of visitor name, time and doors accessed, and name of person contacted.
3. Allow a visitor designation to be assigned to a credential holder.
4. Security access system shall be able to restrict the access levels that may be assigned to credentials issued to visitors.
5. Allow operator to recall visitors' credential-holder file once a visitor is enrolled in the system.
6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.
7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

U. Time and Attendance:

1. Time and attendance reporting shall be provided to match “in” and “out” reads and display cumulative time in for each day and cumulative time in for length designated in the report.
2. Shall be provided to match “in” and “out” reads and display cumulative time in for each day and cumulative time in for length designated in the report.
3. System software setup shall allow designation of selected access-control readers as time and attendance hardware to gather the clock-in and clock-out times of the users at these readers.

    a. Reports shall show in and out times for each day, total time in for each day, and a total time in for period specified by the user.
    b. Allow the operator to view and print the reports, or save the reports to a file.

c. Alphabetically sort reports on the person's last name, by location or location group. Include all credential holders or optionally select individual credential holders for the report.

V. Training Software: Enables operators to practice system operation, including alarm acknowledgment, alarm assessment, response force deployment, and response force communications. System shall continue normal operation during training exercises and shall terminate exercises when an alarm signal is received at the console.

W. Entry-Control Enrollment Software: Database management functions that allow operators to add, delete, and modify access data as needed.

1. The enrollment station shall not have alarm response or acknowledgment functions.
2. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.
3. The program shall provide means to disable the enrollment station when it is unattended, to prevent unauthorized use.
4. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. In the case of personnel identity-verification subsystems, this shall include biometric data. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs. Personnel identity-verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.
5. Cardholder Data: Provide ninety nine (99) user-defined fields. System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features:

   a. Mask: Determines a specific format with which data must comply.
   b. Required: Operator is required to enter data into field before saving.
   c. Unique: Data entered must be unique.
   d. Deactivate Date: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder.
   e. Name ID: Data entered will be considered a unique ID for the cardholder.

6. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.
7. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
8. Batch card printing.

9. Default card data can be programmed to speed data entry for sites where most card data are similar.
10. Enhanced ASCII File Import Utility: Allows the importing of cardholder data and images.
11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

## 2.4 SYSTEM DATABASE

A. Database and database management software shall define and modify each point in database using operator commands. Definition shall include parameters and constraints associated with each system device.

B. Database Operations:

1. System data management shall be in a hierarchical menu-tree format, with navigation through expandable menu branches and manipulated with use of menus and icons in a main menu and system toolbar.
2. Navigational Aids:

    a. Toolbar icons for add, delete, copy, print, capture image, activate, deactivate, and muster report.
    b. Point and click feature to facilitate data manipulation.
    c. Next and previous command buttons visible when editing database fields to facilitate navigation from one (1) record to the next.
    d. Copy command and copy tool in the toolbar to copy data from one record to create a new similar record.

3. Data entry shall be automatically checked for duplicate and illegal data and shall be verified for valid format.
4. System shall generate a memo or note field for each item that is stored in database, allowing the storing of information about any defining characteristics of the item. Memo field is used for noting the purpose for which the item was entered, reasons for changes that were made, and the like.

C. File Management:

1. File management shall include database backup and restoration system, allowing selection of storage media, including 3.5-inch floppy disk, Zip and Jaz drives, and designated network resources.
2. Operations shall be both manual and automatic modes. The number of automatic sequential backups before the oldest backup will be overwritten; FIFO mode shall be operator selectable.
3. Backup program shall provide manual operation from any PC on the LAN and shall operate while system remains operational.

D. Operator Passwords:

1. Support up to [thirty two thousand (32,000)] <Insert number> individual system operators, each with a unique password.
2. [One to eight alphanumeric characters] <Insert password characteristic>.
3. Allow passwords to be case sensitive.
4. Passwords shall not be displayed when entered.
5. Passwords shall have unique and customizable password profile, and allow several operators to share a password profile. Include the following features in the password profile:

   a. Predetermine the highest-level password profile for access to all functions and areas of program.
   b. Allow or disallow operator access to any program operation, including the functions of View, Add, Edit, and Delete.
   c. Restrict doors to which an operator can assign access.

6. Operators shall use a user name and password to log on to system. This user name and password shall be used to access database areas and programs as determined by the associated profile.
7. Make provision to allow the operator to log off without fully exiting program. User may be logged off but program will remain running while displaying the login window for the next operator.

E. Access Card/Code Operation and Management: Access authorization shall be by card, by a manually entered code (PIN), or by a combination of both (card plus PIN).

1. Access authorization shall verify the facility code first, the card or card-and-PIN validation second, and the access level (time of day, day of week, date), anti-passback status, and number of uses last.
2. Use data-entry windows to view, edit, and issue access levels. Access-authorization entry-management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.
3. Allow assignment of multiple cards/codes to a cardholder.
4. Allow assignment of up to four access levels for each Location to a cardholder. Each access level may contain any combination of doors.
5. Each door may be assigned four time zones.
6. Access codes may be up to eleven (11) digits in length.
7. Software shall allow the grouping of locations so cardholder data can be shared by all locations in the group.
8. Visitor Access: Issue a visitor badge for data tracking or photo ID purposes without assigning that person a card or code.
9. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visible annunciation at control station when a selected card or code is used at a designated code reader. Annunciation shall include an automatic display of the cardholder image.

10. Allow each cardholder to be given either an unlimited number of uses or a number from one (1) to nine thousand nine hundred ninety nine (9,999) that regulates the number of times the card can be used before it is automatically deactivated.
11. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.

F. Security Access Integration:

1. Photo ID badging and photo verification shall use the same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.
2. Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.
3. System shall allow sorting of cardholders together by group or other characteristic for a fast and efficient method of reporting on, and enabling or disabling, cards or codes.

G. Key control and tracking shall be an integrated function of cardholder data.

1. Provide the ability to store information about which conventional metal keys are issued and to whom, along with key construction information.
2. Reports shall be designed to list everyone who possesses a specified key.

H. Facility Codes: System shall accommodate up to two thousand forty eight (2,048) facility codes per Location, with the option of allowing facility codes to work at all doors or only at particular doors.

I. Operator Comments:

1. With the press of one appropriate button on the toolbar, the user shall be permitted to enter operator comments into the history at any time.
2. Automatic prompting of operator comment shall occur before the resolution of each alarm.
3. Operator comments shall be recorded by time, date, and operator number.
4. Comments shall be sorted and viewed through reports and history.
5. The operator may enter comments in two ways; either or both may be used:

    a. Manually entered through keyboard data entry (typed), up to sixty five thousand (65,000) characters per each alarm.
    b. Predefined and stored in database for retrieval on request.

6. System shall have a minimum of nine hundred ninety nine (999) predefined operator comments with up to thirty (30) characters per comment.

J. Group:

1. Group names may be used to sort cardholders into groups that allow the operator to determine the tenant, vendor, contractor, department, division, or any other designation of a group to which the person belongs.
2. System software shall have the capacity to assign one of thirty two thousand (32,000) group names to an access authorization.
3. Make provision in software to deactivate and reactivate all access authorizations assigned to a particular group.
4. Allow sorting of history reports and code list printouts by group name.

K. Time Zones:

1. Each zone consists of a start and stop time for seven days of the week and three holiday schedules. A time zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.
2. Up to four time zones may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four (4) lock or unlock periods per day; up to three (3) holiday override schedules may be assigned to a time zone.
3. Data-entry window shall display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.
4. System shall have the capacity for [two thousand forty eight (2,048)] <Insert number> time zones for each Location.

L. Holidays:

1. Three different holiday schedules may be assigned to a time zone. Holiday schedule consists of date in format MM/DD/YYYY and a description. When the holiday date matches the current date of the time zone, the holiday schedule replaces the time-zone schedule for that twenty four (24) hour period.
2. System shall have the capacity for eleven (11) holidays.
3. Three separate holiday schedules may be applied to a time zone.
4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in the system and will not be purged.
5. Holidays not designated to occur each year shall be automatically purged from the database after the date expires.

M. Access Levels:

1. System shall allow for the creation of up to twelve (12) operator accounts and [thirty two thousand (32,000)] <Insert number> access levels.
2. One (1) level shall be predefined as the Master Access Level. The Master Access Level shall work at all doors at all times and override any anti-passback.

3. System shall allow for access to be restricted to any area by reader and by time. Access levels shall determine when and where an Identifier is authorized.
4. System shall be able to create multiple door and time-zone combinations under the same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same controller.

N. User-Defined Fields:

1. System shall provide a minimum of ninety nine (99) user-defined fields, each with up to fifty (50) characters, for specific information about each credential holder.
2. System shall accommodate a title for each field; field length shall be twenty (20) characters.
3. A "Required" option may be applied to each user-defined field that, when selected, forces the operator to enter data in the user-defined field before the credential can be saved.
4. A "Unique" option may be applied to each user-defined field that, when selected, will not allow duplicate data from different credential holders to be entered.
5. Data format option may be assigned to each user-defined field that will require the data to be entered with certain character types in specific spots in the field entry window.
6. A user-defined field, if selected, will define the field as a deactivate date. The selection shall automatically cause the data to be formatted with the windows MM/DD/YYYY date format. The credential of the holder will be deactivated on that date.
7. A search function shall allow any one user-defined field or combination of user-defined fields to be searched to find the appropriate cardholder. The search function shall include a search for a character string.
8. System shall have the ability to print cardholders based on and organized by the user-defined fields.

O. Code Tracing:

1. System shall perform code tracing selectable by cardholder and by reader.
2. Any code may be designated as a "traced code" with no limit to how many codes can be traced.
3. Any reader may be designated as a "trace reader" with no limit to which or how many readers can be used for code tracing.
4. When a traced code is used at a trace reader, the access-granted message that usually appears on the monitor window of the central station shall be highlighted with a different color than regular messages. A short singular beep shall occur at the same time the highlighted message is displayed on the window.
5. The traced cardholder image (if image exists) shall appear on workstations when used at a trace reader.

## 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.

1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."
2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits." as recommended by manufacturer for type of line being protected.

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

## 2.6 DATA GATHERING PANEL

A. All decisions will be made by an intelligent data gathering panel (DGP) located in the designated closets. This panel will be an Lenel Intelligent Controller and boards for the appropriate number of readers, and will meet the following requirements:

1. Make all decisions for the access control system. The host computer software functions primarily to collect transactions and program the system. All real decisions are made at the DGP.
2. Incorporate flash memory, eliminating the need to change firmware. All software updates for the DGP will be achieved via flash memory.
3. Be network compatible with the hospital's existing network.
4. Be supported by two UL-Listed Power Supplies providing a minimum 4 hours of battery backup for the locks, readers and peripheral devices.
5. The power supplies will incorporate individually fused lock outputs, and will be the Altronix AL1024ULACM and AL1012ULACM or approved equal.

B. All card readers will be wired in a star configuration. The alternative daisy-chain configuration is not acceptable. All card readers, REXes and locking hardware will be powered at power supplies located at designated closet location.

## 2.7 CENTRAL-STATION HARDWARE

A. Central-Station Computer: Standard unmodified PC of modular design. The CPU word size shall be thirty two (32) bytes or larger; the CPU operating speed shall be at least 2.0 GHz.

1. Memory: [256] <Insert number> MB of usable installed memory, expandable to a minimum of [1024] <Insert number> MB without additional chassis or power supplies.
2. Power Supply: Minimum capacity of [250] <Insert number> W.
3. Real-Time Clock:

    a. Accuracy: Plus or minus one minute per month.
    b. Time-Keeping Format: twenty four (24) hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
    c. Clock shall function for one year without power.
    d. Provide automatic time correction once every twenty four (24) hours by synchronizing clock with the Time Service Department of the U.S. Naval Observatory.

4. Serial Ports: Provide two TIA 232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
5. Parallel Port: An enhanced parallel port.
6. LAN Adapter Card: 10/100 Mbps PCI bus, internal network interface card.
7. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.
8. Color Monitor: Not less than seven teen (17) inches, with a minimum resolution of 1280 by 1024 pixels, noninterlaced, and a maximum dot pitch of 0.28 mm. The video card shall support at least 256 colors at a resolution of 1280 by 1024 at a minimum refresh rate of 70 Hz.
9. Keyboard: With a minimum of sixty four (64) characters, standard ASCII character set based on ANSI INCITS 154.
10. Mouse: Standard, compatible with the installed software.
11. Special-function keyboard attachments or special-function keys to facilitate data input of the following operator tasks:

    a. Help.
    b. Alarm Acknowledge.
    c. Place Zone in Access.
    d. Place Zone in Secure.
    e. System Test.
    f. Print Reports.
    g. Change Operator.
    h. <Insert operator tasks>.

12. Disk storage shall include the following, each with appropriate controller:

    a. Minimum 10 GB hard disk, maximum average access time of ten (10) ms.
    b. Floppy Disk Drive: High density, three and one half (3-1/2) inch size.
    c. PCMCIA slot with removable 500 MB media.
    d. 100 MB Iomega Zip drive.
    e. 250 MB Iomega Jaz drive.

13. Magnetic Tape System: 4-mm cartridge magnetic tape system with minimum [2] [4] [12] [20] GB <Insert number> formatted capacity per tape. Provide ten (10) tapes, each in a rigid cartridge with spring-loaded cover and operator-settable write-protect feature.
14. Modem: Fifty six thousand six hundred (56,600) bps, full duplex for asynchronous communications. With error detection, auto answer/autodial, and call-in-progress detection. Modem shall comply with requirements in ITU-T V.34, ITU-T V.42 for error correction, and ITU-T V.42 BIS for data compression standards; and shall be suitable for operating on unconditioned voice-grade telephone lines complying with 47 CFR 68.
15. Audible Alarm: Manufacturer's standard.
16. CD-ROM Drive:

    a. Nominal storage capacity of 650 MB.
    b. Data Transfer Rate: 1.2 Mbps.
    c. Average Access Time: 150 ms.
    d. Cache Memory: 256 KB.
    e. Data Throughput: 1 MB/second, minimum.

17. Dot Matrix Alarm Printer:

    a. Connected to the central station.
    b. Minimum of 96 characters, standard ASCII character set based on ANSI INCITS 154, and with graphics capability and programmable top-of-form control.
    c. Prints in both red and black without ribbon change.
    d. Adjustable sprockets for paper width up to eleven (11) inches.
    e. 80 columns per line, minimum speed of two hundred (200) characters per second.
    f. Character Spacing: Selectable at ten (10), twelve (12), or seventeen (17) characters per inch.
    g. Paper: Sprocket-fed fan fold paper.

18. Report Printer:

    a. Connected to the central station and designated workstations.
    b. Laser printer with minimum resolution of 600 dpi.
    c. RAM: 2 MB, minimum.

d. Printing Speed: Minimum twelve (12) pages per minute.
e. Paper Handling: Automatic sheet feeder with two hundred fifty (250) sheet paper cassette and with automatic feed.

19. Interface: Bidirectional parallel, and universal serial bus.
20. LAN Adapter Card: 10/100 Mbps internal network interface card.

B. Redundant Central Computer: One identical redundant central computer, connected in a hot standby, peer configuration. This computer shall automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files shall be updated to system files of redundant computer in near real time. If central computer fails, redundant computer shall assume control immediately and automatically.

C. UPS: Self-contained; complying with requirements in Division 26 Section "Static Uninterruptible Power Supply."

1. Size: Provide a minimum of four (4) hours of operation of the central-station equipment, including two hours of alarm printer operation.
2. Batteries: Sealed, valve regulated, recombinant, lead calcium.
3. Accessories:

a. Transient voltage suppression.
b. Input-harmonics reduction.
c. Rectifier/charger.
d. Battery disconnect device.
e. Static bypass transfer switch.
f. Internal maintenance bypass/isolation switch.
g. External maintenance bypass/isolation switch.
h. Output isolation transformer.
i. Remote UPS monitoring.
j. Battery monitoring.
k. Remote battery monitoring.

## 2.8 STANDARD WORKSTATION HARDWARE

A. Workstation shall consist of a standard unmodified PC with accessories and peripherals that configure the workstation for a specific duty.

B. Workstation Computer: Standard unmodified PC of modular design. The CPU word size shall be thirty two (32) bytes or larger; the CPU operating speed shall be at least 2.0 GHz.

1. Memory: 512 MB of usable installed memory, expandable to a minimum of 8 GB without additional chassis or power supplies.
2. Power Supply: Minimum capacity of 250 W.

3. Real-Time Clock:

   a. Accuracy: Plus or minus one minute per month.
   b. Time-Keeping Format: Twenty four (24) hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
   c. Provide automatic time correction once every twenty four (24) hours by synchronizing clock with the central station.

4. Serial Ports: Provide two TIA 232-F USB serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
5. Parallel Port: An enhanced parallel port.
6. Sound Card: For playback and recording of digital WMP sound files that are associated with audible warning and alarm functions.
7. Color Monitor: Not less than seventeen (17) inches, with a minimum resolution of 1280 by 1024 pixels, noninterlaced, and a maximum dot pitch of 0.28 mm. The video card shall support at least 256 colors at a resolution of 1280 by 1024 at a minimum refresh rate of 70 Hz.
8. Keyboard: With a minimum of sixty four (64) characters, standard ASCII character set based on ANSI INCITS 154.
9. Mouse: Standard, compatible with the installed software. Minimum resolution shall be 400 dpi.
10. Disk storage shall include the following, each with appropriate controller:

    a. Minimum 20 GB hard disk, maximum average access time of ten (10) ms.
    b. Floppy Disk Drive: High density, three and one half (3-1/2) inch size.

11. CD-ROM/CD-RW Drive:

    a. Nominal Storage Capacity: 700 MB.
    b. Data Transfer Rate: 3.6 Mbps.
    c. Average Access Time: 150 ms.
    d. Cache Memory: 512 KB.
    e. Data Throughput: 3.6 MB/second, minimum.
    f. Read Speed: 48x.
    g. Write Speed: 32x.

12. DVD/DVD-RW Drive:

    a. Nominal Storage Capacity: 4.7 GB.
    b. Data Transfer Rate: 3.6 Mbps.
    c. Cache Memory: 512 KB.
    d. Read Speed: 24x.
    e. Write Speed: 6x.

13. Printer:

a. Connected to the central station and designated workstations.
b. Laser printer with minimum resolution of 600 dpi.
c. RAM: 8 MB, minimum.
d. Printing Speed: Minimum twelve (12) pages per minute.
e. Paper Handling: Automatic sheet feeder with two hundred fifty (250) sheet paper cassette and with automatic feed.

14. Interface: Bidirectional parallel, and universal serial bus.
15. LAN Adapter Card: 10/100 Mbps internal network interface card.

C. Redundant Workstation: One identical redundant workstation, connected in a hot standby, peer configuration. This workstation shall automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files shall be updated to system files of redundant workstation in near real time. If its associated workstation fails, redundant workstation shall assume control immediately and automatically.

D. UPS: Self-contained, complying with requirements in Division 26 Section "Static Uninterruptible Power Supply."

1. Size: Provide a minimum of four (4) hours of operation of the central-station equipment, including two hours of alarm printer operation.
2. Batteries: Sealed, valve regulated, recombinant, lead calcium.
3. Accessories:

a. Transient voltage suppression.
b. Input-harmonics reduction.
c. Rectifier/charger.
d. Battery disconnect device.
e. Static bypass transfer switch.
f. Internal maintenance bypass/isolation switch.
g. External maintenance bypass/isolation switch.
h. Output isolation transformer.
i. Remote UPS monitoring.
j. Battery monitoring.
k. UPS operation monitoring.
l. Abnormal operation. Visible and audible indication.
m. Remote battery monitoring.
n. <Insert accessories>.

## 2.9 COMMUNICATIONS WORKSTATION

A. Standard workstation, modified as follows:

1. Two additional TIA 232-F serial port(s). The CPU word size shall be 32 bytes or larger; the CPU operating speed shall be at least 2.0 GHz. Multiplexed serial ports shall be expandable with eight-character transmit and receive buffers for each port. Total-buffer size shall be a minimum of 1 MB.
2. Redundant workstation is not required.
3. Printer is not required.

## 2.10 FIXED MAP DISPLAY

A. A fixed map display shall show layout of the protected facilities. Zones corresponding to those monitored by the system shall be highlighted on the display. Status of each zone shall be displayed using digital displays as required within each designated zone. A digital display test switch shall be provided on the map display.

## 2.11 CONTROLLERS

A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the central station or workstation for controlling its operation.

B. Subject to compliance with requirements in this article, manufacturers may use multipurpose controllers.

C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of four (4) hours, complying with UL 924.

D. Alarm Annunciation Controller:

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

    a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.
    b. Alarm-Line Supervision:

        1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal, and for conditions as described in UL 1076 for line security equipment by monitoring for abnormal open, grounded, or shorted conditions using dc change measurements. System shall initiate an alarm in response to an abnormal current, which is a dc change of 10 % or more for longer than five hundred (500) ms.

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

c. Outputs: Managed by central-station software.

2. Auxiliary Equipment Power: A GFI service outlet inside the controller enclosure.

E. Entry Controller:

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

a. Operate as a stand-alone portal controller using the downloaded database during periods of communication loss between the controller and the field-device network.

b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:

1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.

2) Privileges shall include, but are not limited to, time of day control, day of week control, group control, and visitor escort control.

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

## 2.12 READER AND DOOR OPERATION

A. The card reader door, the system shall have the following operational capability:

1. Readers shall read cards while the door is in the open position.
2. Door shall lock automatically upon the door being opened.
3. Automatic locking of the door lock after the door has been opened can be delayed for a user-defined time period.
4. Alarm from the door shall be shunted following the presentation of a valid access card, activation of the request to exit device and/or the pressing of the exit button.
5. Shall include a separate (alternate) shunt timer to extend the door shunt time after an access granted access occurs when a valid card has been presented by an

individual with special ADA requirements. This will be determined as a check box in that cardholder's card record, and will be user definable.

6. Each card reader door shall be monitored for both forced and propped open conditions. The system shall differentiate between the two types of conditions, and notify the alarm monitoring center of each specific alarm condition, initiating a different response for each alarm type.
7. All door locks for stairwells and exits shall have a master over-ride switch which will be placed at the Main Fire Control Panel location.
8. Inputs:

    a. Data from entry-control devices; use this input to change modes between access and secure.
    b. Database downloads and updates from the central station that include enrollment and privilege information.

9. Outputs:

    a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.
    b. Grant or deny entry by sending control signals to portal-control devices and mask intrusion-alarm annunciation from sensors stimulated by authorized entries.
    c. Maintain a date-, time-, and Location-stamped record of each transaction and transmit transaction records to the central station.
    d. Door Prop Alarm: If a portal is held open for longer than time listed in a schedule, alarm sounds.

10. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
11. Data Line Problems: For periods of loss of communication with the central station, or when data transmission is degraded and generating continuous checksum errors, the controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.

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

12. Controller Power: NFPA 70, Class II power-supply transformer, with 12- or 24-V ac secondary, backup battery and charger.

    a. Backup Battery: Premium, valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full one (1) year warranty and a pro rata [19] [9]-year warranty. With single-stage, constant-voltage-current,

limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.

b. Backup 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.

c. Backup Power-Supply Capacity: Four (4) hours of battery supply. Submit battery and charger calculations.

d. Power Monitoring: Provide manual, dynamic battery-load test, initiated and monitored at the control center; with automatic disconnection of the controller when battery voltage drops below controller limits. Report by using local controller-mounted digital displays and by communicating status to central station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:

1) Trouble Alarm: Normal power-off load assumed by battery.
2) Trouble Alarm: Low battery.
3) Alarm: Power off.

## 2.13 SECONDARY ALARM ANNUNCIATOR

A. Secondary Alarm Annunciation Site: A workstation with limited I/O capacity, consisting of a secondary alarm annunciation workstation to allow the operator to duplicate functions of the main operator interface and to show system status changes.

## 2.14 CARD READERS, CREDENTIAL CARDS, AND KEYPADS

A. Card-Reader Power: Powered from its associated controller, including its standby power source, and shall not dissipate more than 5 W.

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

C. Enclosure: Suitable for surface, semi-flush, pedestal, or weatherproof 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 needed for operation at the site.

D. Display: Digital visual indicator shall provide visible and audible status indications and user prompts. Indicate power on or off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

E. Touch-Plate and Proximity Readers:

1. The system shall use proximity readers manufactured by HID, and will use the "Thinline" series model of reader. Other manufacturers and product types are not acceptable.
2. Passive-detection proximity card readers shall use a swept-frequency, RF field generator to read the resonant frequencies of tuned circuits laminated into compatible credential cards. The resonant frequencies read shall constitute a unique identification code number.
3. The card reader shall read proximity cards in a range from direct contact to at least 6 inches from the reader.

F. Communication Protocol: Compatible with local processor.

G. Touch-Plate and Contactless Card Reader: The reader shall have "flash" download capability to accommodate card format changes. The card reader shall have capability of transmitting data to security control panel and shall comply with ISO/IEC 7816.

H. Credential Card Modification: Entry-control cards shall be able to be modified by lamination direct print process during the enrollment process without reduction of readability. The design of the credential cards shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the badge holder used at the site.

I. Card Size and Dimensional Stability: Credential cards shall be 2-1/8 by 3-3/8 inches. The credential card material shall be dimensionally stable so that an undamaged card with deformations resulting from normal use shall be readable by the card reader.

J. Card Material: Abrasion resistant, nonflammable, nontoxic, and impervious to solar radiation and effects of ultraviolet light.

K. Card Construction:

1. Core and laminate or monolithic construction.
2. Lettering, logos, and other markings shall be hot stamped into the credential material or direct printed.
3. Incorporate holographic images as a security enhancement.
4. Furnish equipment for on-site assembly and lamination of credential cards.

## 2.15 PHOTO-IDENTIFICATION AND BADGING SYSTEM (PIB)

A. As part of this system, the university shall be provided with an integrated photo-identification and badging system. The photo-badging system shall meet the following requirements:

1. Be an integral part of the access control system. Every cardholder record in the access control system shall display the stored image of the cardholder in their personnel record. The system shall be an embedded part of the access control system.
2. The PIB shall operate on the same client/server architecture as the access control system. The images shall be stored in a central server and shall be available to all authorized operator workstations.
3. Use an image capture board with a single-slot, high performance, PCI bus accelerated, twenty four (24) bpp true-color Super VGA frame grabber designed to capture and display high quality video images. The image capture card shall contain a minimum 2MB DRAM, and shall provide a complete set of camera control functions required for capturing high quality video images. Video shall be captured by connecting an NTSC or PAL video source to the capture board's composite or S-Video input. The capture board shall be capable of displaying live video in a window. Software adjustable controls (hue, saturation, brightness, contrast, offset and gain) shall be controllable through the video imaging application.
4. Images shall be stored in industry standard graphics formats, including JPEG, TIFF, TARGA, PCX, BMP, WMF and PICT. The system shall allow images of the various formats to be stored and displayed by operator workstations.
5. The PIB shall include a complete identification badge design and layout tool, and shall make use of a what-you-see-is-what-you-get (WYSIWYG) editor, including drag and drop placement. The operator shall use the mouse to size image and text object fields, dragging the layout box in both horizontal and vertical directions. The mouse shall also be used to move objects around on the badge layout. The contractor will create several badge formats for the hospital.
6. Provide high-resolution cameras to capture the images into the system.
7. Provide a printer and all of the necessary supplies to badge 1000 cardholders.

B. Enrollment equipment shall support encoding of credential cards including cryptographic and other internal security checks as required for system.

1. Allow only authorized entry-control enrollment personnel to access the enrollment equipment using passwords.
2. Include enrollment-subsystem configuration controls and electronic diagnostic aids for subsystem setup and troubleshooting with the central station.
3. Enrollment-station records printer shall meet requirements of the report printer.

C. Entry-Control Enrollment Software:

1. Shall include database management functions for the system, and shall allow an operator to change and modify the data entered in the system as needed.

2. Software shall not have alarm response or acknowledgment functions as a programmable function.
3. Multiple, password-protected access levels shall be provided at the enrollment station.
4. Database management and modification functions shall require a higher operator-access level than personnel enrollment functions.
5. Software shall provide a means for disabling the enrollment station when it is unattended, to prevent unauthorized use.
6. Software shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations to include a credential unit in use at the installation.
7. In the case of personnel identity-verification subsystems, this data shall include biometric data.
8. Software shall allow entry of this data into the system database files through the use of simple menu selections and data fields. The data field names shall be customized to suit user and site needs.
9. Personnel identity-verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.

D. Accessories:

1. Steel desk-type console, swivel chair on casters, and equipment racks.
2. Console and Equipment Racks: Comply with EIA/ECA-310-E.
3. Equipment, with the exception of the printers, shall be rack mounted in the console and equipment racks.
4. Storage Cabinet: Locking cabinet approximately seventy two (72) inches high, thirty six (36) inches wide, and twenty four (24) inches deep, with three adjustable shelves and two storage racks for storage of disks, tapes, printouts, printer paper, ribbons, manuals, and other documentation.

E. System Capacity: Number of badges shall be limited only by hard disk space. Badge templates and images shall be in color, supporting the maximum color capability of Microsoft Windows.

F. Badge Configuration:

1. Software for badge template creation shall include a template consisting of background and predetermined locations of photographs, text objects and data fields for text, and bar-code and biometric information. Include automatic sizing of data fields placed on a badge to compensate for names, which may otherwise be too large to fit in the area designated.
2. Allow different badge templates to be used for each department, tenant, or visitor.
3. As a setup option, templates shall be automatically selected for the badge, based on the group to which the credential holder is assigned. Allow the operator to

override the automatic template selection and use a template chosen by the operator for creating a badge.

4. Setup shall determine which graphics and credential-holder information will be displayed and where on the card it will be placed. All data in the security access system, such as name, code, group, access level, and any of the ninety nine (99) user-defined fields, shall be selectable, with the ability to place them anywhere on the card.
5. System shall include an importing, filing, and recall system of stored images and shapes that can be placed on the badge.
6. Allow multiple images on the same badge, including, but not limited to, bar codes, digital photos, and signatures.
7. Support transparent backgrounds so that image is only surrounded by the intended background and not by its immediate background.

G. Photo Imaging: Integral to security access.

1. Import images from bitmap file formats, digital cameras, TWAIN cameras, or scanners. Allow image cropping and editing, WYSIWYG badge-building application, and badge print-preview and printing capabilities.
2. System shall support multiple images stored for each credential holder, including signatures, portrait views, and profile views.

H. Text Objects: Badge configuration shall provide for creation of custom text as an object, allowing font selection, typing, scaling, and formatting of the text object. Formatting options shall include changing font, font size, text flow, and text alignment; bending or curving the text object into a circle or semicircle; applying 3-D effects; and applying predefined effects such as tilt, extrusion, or beveling. Text shall be placed and optionally automatically centered within any region of the badge layout.

I. Badges and Credential Cards:

1. Badges are credential cards that do not contain data to be read by card readers.
2. Credential cards shall store uniquely coded data used by card readers as an Identifier.

    a. Proximity Cards: Use proximity detection without physical contact with the reader for proper operation.

3. Allow entry-control card to be modified by lamination or direct print process during the enrollment process for use as a picture and identification badge without reduction of readability. The design shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the type of badge holder used at the site.

    a. Card Size and Dimensional Stability: Standard size, two and one eighth (2-1/8) by three and three eighths (3-3/8) inches; dimensionally stable so that

an undamaged card with deformations resulting from normal use shall be readable by the card reader.

b. Card Material: Abrasion resistant, nonflammable, and nontoxic; and impervious to solar radiation and effects of ultraviolet light.

c. Card Construction: Core and laminate or monolithic construction. Lettering, logos, and other markings shall be hot stamped into the credential material or direct printed.

1) Incorporate holographic images as a security enhancement.
2) Furnish equipment for on-site assembly and lamination of credential cards.

d. Card Durability and Maintainability: Designed and constructed to yield a useful lifetime of at least five (5) years or five thousand (5,000) insertions or swipes, whichever results in a longer period of time. Allow credential cards to be cleaned by wiping with a sponge or cloth wetted with soap and water.

J. Card-Making Equipment: Consisting of a workstation, video camera, video-imaging equipment, and a printer.

1. Camera: NTSC color standard, RGB video output, 470 lines minimum horizontal resolution, and automatic white balance with full rated output under illumination of 0.5 fc.
2. Video Imaging: Live-image capture software and hardware and a digital signature capture pad.
3. Standard workstation, modified as follows:

a. Redundant workstation is not required.
b. Printer is not required.
c. UPS is not required.
d. Sound card is not required.

4. Printer: Dye-sublimation resin thermal transfer, 300 dpi resolution, 16.7 million colors, accepting cards ranging in size from 2.1 by 3 inches to 2.6 by 3.7 inches and having card thickness ranging from 0.020 to 0.060 inch. Printer shall have options for encoding magnetic stripe using tracks 1, 2, and 3. Throughput shall be not less than 60 seconds per card.

## 2.16 PUSH-BUTTON SWITCHES

A. Push-Button Switches: Momentary-contact back-lighted push buttons with stainless-steel switch enclosures.

B. Electrical Ratings:

1. Minimum continuous current rating of 10 A at 120-V ac or 5 A at 240-V ac.
2. Contacts that will make 720 VA at 60 A and that will break at 720 VA at 10 A.

C. Enclosures: Flush or surface mounting. Push buttons shall be suitable for flush mounting in the switch enclosures.

D. Enclosures shall additionally be suitable for installation in the following locations:

1. Indoors, controlled environment.
2. Indoors, uncontrolled environment.
3. Outdoors.

E. Power: Push-button switches shall be powered from their associated controller, using dc control.

## 2.17 DOOR AND GATE HARDWARE INTERFACE

A. Exit Device with Alarm: Operation of the exit device shall generate an alarm and annunciate a local alarm. Exit device and alarm contacts are specified in Division 08 Section "Door Hardware."

1. Request to Exit Devices. Each card reader door will be equipped with a REX device manufactured by DSI. This will be a DSI 150I, and will enable the system to both differentiate and monitor the door for forced and prop open conditions.
2. Door Contacts. The status of each card reader door will be monitored with a magnetic door contact. This will be a Sentrol 1078C-W wide-gapped contact, no exceptions.

B. Exit Alarm: Operation of a monitored door shall generate an alarm. Exit devices and alarm contacts are specified in Division 08 Section "Door Hardware."

C. Electric Door Strikes: Use end-of-line resistors to provide power-line supervision. Signal switches shall transmit data to controller to indicate when the bolt is not engaged and the strike mechanism is unlocked, and they shall report a forced entry. Power and signal shall be from the controller. Electric strikes are specified in Division 08 Section "Door Hardware."

D. Electromagnetic Locks: End-of-line resistors shall provide power-line supervision. Lock status sensing signal shall positively indicate door is secure. Power and signal shall be from the controller. Electromagnetic locks are specified in Division 08 Section "Door Hardware."

E. Vehicle Gate Operator: Interface electrical operation of gate with controls in this Section. Vehicle gate operators shall be connected, monitored, and controlled by the security

access controllers. Vehicle gate and accessories are specified in Division 32 Section "Chain Link Fences and Gates."

## 2.18 FIELD-PROCESSING SOFTWARE

A. Operating System:

1. Local processors shall contain an operating system that controls and schedules that local processor's activities in real time.
2. Local processor shall maintain a point database in its memory that includes parameters, constraints, and the latest value or status of all points connected to that local processor.
3. Execution of local processor application programs shall utilize the data in memory resident files.
4. Operating system shall include a real-time clock function that maintains the seconds, minutes, hours, date, and month, including day of the week.
5. Local processor real-time clock shall be automatically synchronized with the central station at least once per day to plus or minus ten (10) seconds (the time synchronization shall be accomplished automatically, without operator action and without requiring system shutdown).

B. Startup Software:

1. Causes automatic commencement of operation without human intervention, including startup of all connected I/O functions.
2. Local processor restart program based on detection of power failure at the local processor shall be included in the local processor software.
3. Initiates operation of self-test diagnostic routines.
4. Upon failure of the local processor, if the database and application software are no longer resident, the local processor shall not restart and systems shall remain in the failure mode indicated until the necessary repairs are made.
5. If the database and application programs are resident, the local processor shall immediately resume operation.

C. Operating Mode:

1. Local processors shall control and monitor inputs and outputs as specified, independent of communications with the central station or designated workstations.
2. Alarms, status changes, and other data shall be transmitted to the central station or designated workstations when communications circuits are operable.
3. If communications are not available, each local processor shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the central station or designated workstations, shall be stored for later transmission to the central station or designated workstations.

4. Storage for the latest four thousand (4,000) events shall be provided at local processors, as a minimum.
5. Local processors shall accept software downloaded from the central station.
6. Panel shall support flash ROM technology to accomplish firmware downloads from a central location.

D. Failure Mode: Upon failure for any reason, each local processor shall perform an orderly shutdown and force all local processor outputs to a predetermined (failure-mode) state, consistent with the failure modes shown and the associated control device.

E. Functions:

1. Monitoring of inputs.
2. Control of outputs.
3. Reporting of alarms automatically to the central station.
4. Reporting of sensor and output status to central station upon request.
5. Maintenance of real time, automatically updated by the central station at least once a day.
6. Communication with the central station.
7. Execution of local processor resident programs.
8. Diagnostics.
9. Download and upload data to and from the central station.

## 2.19 FIELD-PROCESSING HARDWARE

A. Alarm Annunciation Local Processor:

1. Respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station, and change outputs based on commands received from the central station.
2. Local processor shall also automatically restore communication within 10 seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs.
3. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions.
4. Local processor shall have at least eight (8) alarm inputs which allow wiring contacts as normally open or normally closed for alarm conditions; and shall provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements.
5. Local processor shall report line supervision alarms to the central station.
6. Alarms shall be reported for any condition that remains abnormal at an input for longer than 500 milliseconds.
7. Alarm condition shall be transmitted to the central computer during the next interrogation cycle.

8. Local processor outputs shall reflect the state of commands issued by the central station.
9. Outputs shall be a form C contact and shall include normally open and normally closed contacts.
10. Local processor shall have at least four command outputs.
11. Local processor shall be able to communicate with the central station via RS-485 or TCP/IP as a minimum.

B. Processor Power Supply:

1. Local processor and sensors shall be powered from an uninterruptible power source.
2. Uninterruptible power source shall provide eight hours of battery back-up power in the event of primary power failure and shall automatically fully recharge the batteries within twelve (12) hours after primary power is restored.
3. If the facility is without an emergency generator, the uninterruptible power source shall provide twenty four (24) hours of battery backup power.
4. There shall be no equipment malfunctions or perturbations or loss of data during the switch from primary to battery power and vice versa.
5. Batteries shall be sealed, non-out gassing type.
6. Power supply shall be equipped with an indicator for ac input power and an indicator for dc output power.
7. Loss of primary power shall be reported to the central station as an alarm.

C. Auxiliary Equipment Power: A GFI service outlet shall be furnished inside the local processor's enclosure.

D. Entry-Control Local Processor:

1. Entry-control local processor shall respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station, and change outputs based on commands received from the central station.
2. Local processor shall also automatically restore communication within ten (10) seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs.
3. Entry-control local processor shall provide local entry-control functions including communicating with field devices such as card readers, keypads, biometric personnel identity-verification devices, door strikes, magnetic latches, gate and door operators, and exit push buttons.
4. Processor shall also accept data from entry-control field devices as well as database downloads and updates from the central station that include enrollment and privilege information.
5. Processor shall send indications of successful or failed attempts to use entry-control field devices and shall make comparisons of presented information with stored identification information.

6. Processor shall grant or deny entry by sending control signals to portal-control devices and mask intrusion-alarm annunciation from sensors stimulated by authorized entries.
7. Entry-control local processor shall use inputs from entry-control devices to change modes between access and secure.
8. Local processor shall maintain a date-time- and location-stamped record of each transaction and transmit transaction records to the central station.
9. Processor shall operate as a stand-alone portal controller using the downloaded database during periods of communication loss between the local processor and the central station.
10. Processor shall store a minimum of four thousand (4,000) transactions during periods of communication loss between the local processor and the central station for subsequent upload to the central station upon restoration of communication.
11. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions.
12. Local processor shall have at least eight alarm inputs which allow wiring contacts as normally open or normally closed for alarm conditions; and shall also provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements.
13. Local processor shall report line supervision alarms to the central station.
14. Alarms shall be reported for any condition that remains abnormal at an input for longer than 500 ms.
15. Alarm condition shall be transmitted to the central station during the next interrogation cycle.
16. Entry-control local processor shall include the necessary software drivers to communicate with entry-control field devices. Information generated by the entry-control field devices shall be accepted by the local processor and automatically processed to determine valid identification of the individual present at the portal.
17. Upon authentication of the credentials or information presented, the local processor shall automatically check privileges of the identified individual, allowing only those actions granted as privileges.
18. Privileges shall include, but are not limited to, time of day control, day of week control, group control, and visitor escort control. The local processor shall maintain a date-time- and location-stamped record of each transaction.
19. Transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.
20. Local processor outputs shall reflect the state of commands issued by the central station.
21. Outputs shall be a form C contact and shall include normally open and normally closed contacts.
22. Local processor shall have at least four addressable outputs.
23. The entry-control local processor shall also provide control outputs to portal-control devices.

24. Local processor shall be able to communicate with the central station via RS-485 or TCP/IP as a minimum.
25. The system manufacturer shall provide strategies for downloading database information for panel configurations and cardholder data to minimize the required download time when using IP connectivity.

## 2.20 TIA 232-F ASCII INTERFACE SPECIFICATIONS

A. ASCII interface shall allow TIA 232-F connections to be made between the control station operating as the host PC and any equipment that will accept TIA 232-F ASCII command strings, such as CCTV switches, intercoms, and paging systems.

1. Alarm inputs in system shall allow for individual programming to output up to four unique ASCII character strings through two different COM ports on the host PC.
2. Inputs shall have the ability to be defined to transmit a unique ASCII string for alarm and one for restore through one COM port, and a unique ASCII string for a nonalarm, abnormal condition and one for a normal condition through the same or different COM port.
3. Predefined ASCII character strings shall have the ability to be up to 420 characters long with full use of all the ASCII control characters, such as return or line feed. Character strings shall be defined in the system database and then assigned to the appropriate inputs.
4. COM ports of the host PC used to interface with external equipment shall be defined in the setup portion of the software. COM port's baud rate, word length, stop bits, and parity shall be definable in the software to match that of the external equipment.

B. Pager-System Interface: Alarms shall be able to activate a pager system with customized message for each input alarm.

1. TIA 232-F output shall be capable of connection to a pager interface that can be used to call a paging system or service and send a signal to a portable pager. System shall allow an individual alphanumeric message per alarm input to be sent to the paging system. This interface shall support both numeric and alphanumeric pagers.

C. Alarm-System Interface:

1. TIA 232-F output shall be capable of transmitting alarms from other monitoring and alarm systems to central-station automation software.
2. Alternatively, alarms that are received by this access-control system are to be transferred to the alarm automation system as if they were sent through a digital alarm receiver.

a. System shall be able to transmit an individual message from any alarm input to a burglar-alarm automation monitoring system.
b. System shall be able to append to each message a predefined set of character strings as a prefix and a suffix.

## 2.21 FLOOR-SELECT ELEVATOR CONTROL

A. Elevator access control shall be integral to security access.

1. System shall be capable of providing full elevator security and control through dedicated controllers without relying on the control-station host PC for elevator control decisions.
2. Access-control system shall enable and disable car calls on each floor and floor-select buttons in each elevator car, restricting passengers' access to the floors where they have been given access.
3. System setup shall, through programming, automatically and individually secure and unsecure each floor-select button of a car by time and day. Each floor-select button within a car shall be separately controlled so that some floors may be secure while others remain unsecure.
4. When a floor-select button is secure, it shall require the passenger to use his or her access code and gain access to that floor before the floor-select button will operate. The passenger's credential shall determine which car call and floor-select buttons are to be enabled, restricting access to floors unless authorized by the system's access code database. Floor-select button shall be enabled only in the car where the credential holder is the passenger.

B. Security access system shall record which call button is pressed, along with credential and time information.

1. System controller shall record elevator access data.
2. The controller shall reset all additional call buttons that may have been enabled by the user's credential.
3. The floor-select elevator control shall allow for manual override from a workstation PC either by individual floor or by cab.

## 2.22 REAL-TIME GUARD TOUR

A. Guard tour module shall provide the ability to plan, track, and route tours. Module shall input an alarm during tour if guard fails to make a station. Tours can be programmed for sequential or random tour-station order.

1. Guard tour setup shall define specific routes or tours for the guard to take, with time restrictions in which to reach every predefined tour station.

2. Guard tour activity shall be automatically logged to the central-station PC's hard drive.
3. If the guard is early or late to a tour station, a unique alarm per station shall appear at the central station to indicate the time and station.
4. Guard tour setup shall allow the tours to be executed sequentially or in a random order with an overall time limit set for the entire tour instead of individual times for each tour station.
5. Setup shall allow recording of predefined responses that will display for the operator at the control station should a "Failed to Check In" alarm occur.

B. Guard tour module shall allow proprietary direct-connected systems to use security access-control hardware to perform guard tour management in real time.

C. A tour station is a physical location where a guard shall go and perform an action indicating that he or she has arrived. This action, performed at the tour station, shall be one of 13 different events with any combination of station types within the same tour. An event at a tour station shall be one of the following types:

1. Access Granted.
2. Access Denied Code.
3. Access Denied Card plus PIN.
4. Access Denied Time Zone.
5. Access Denied Level.
6. Access Denied Facility.
7. Access Denied Code Timer.
8. Access Denied Anti-Passback.
9. Access Granted Passback Violation.
10. Alarm.
11. Restored.
12. Input Normal.
13. Input Abnormal.

D. Guard tour and other system features shall operate simultaneously with no interference.

E. Guard Tour Module Capacity: Nine hundred ninety nine (999) possible guard tour definitions with each tour having up to ninety nine (99) tour stations. System shall allow all nine hundred ninety nine (999) tours to be running at the same time.

## 2.23 VIDEO AND CAMERA CONTROL

A. Control station or designated workstation displays live video from a CCTV source.

1. Control Buttons: On the display window, with separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan, and a minimum of two custom-command auxiliary controls.

2. Provide at least seven icons to represent different types of cameras, with ability to import custom icons. Provide option for display of icons on graphic maps to represent their physical location.
3. Provide the alarm-handling window with a command button that will display the camera associated with the alarm point.

B. Display mouse-selectable icons representing each camera source, to select source to be displayed. For CCTV sources that are connected to a video switcher, control station shall automatically send control commands through a COM port to display the requested camera when the camera icon is selected.

C. Allow cameras with preset positioning to be defined by displaying a different icon for each of the presets. Provide control with Next and Previous buttons to allow operator to cycle quickly through the preset positions.

## 2.24 EMERGENCY PHONE EXTERIOR

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following available manufacturers offering products that may be incorporated into the Work include, but are limited to, the following:

1. Code Blue

B. Exterior Code Blue telephones require power and voice cables ran to them.

C. Exterior Code Blue telephone pole units are required to have ventilation.

D. Exterior Code Blue pole telephones are to be Model CB 5-S. The color of the pole is to be blue and the wording is to be white.

1. Code Blue CB 5 shall be an easily identifiable, vandal resistant communications device that is Americans with Disabilities Act (ADA) compliant, multi-functional, freestanding, and constructed of heavy steel. The unit shall be aesthetically pleasing and almost impervious to damage, and include a high quality, vandal resistant, hands-free communications device, and a powerful combination blue strobe and beacon that serve to identify the unit from a great distance.
2. The Code Blue CB3100 communication system shall be designed so that a single touch on the communications device button shall immediately and automatically dial a preprogrammed number. This shall simultaneously activate the blue strobe light and an optional peripheral device such as a remote preset for closed circuit television (CCTV). Immediately after establishing the phone connection with the receiving party, the communications device shall be capable of sending a signal identifying the specific unit being activated. The strobe shall continue to flash, drawing attention to the location until the receiving party terminates the call.
3. Construction

a. The housing shall be a concentric steel cylinder (bollard) with a 8.75 inch diameter, a .25 inch wall thickness and a height of 113.5 inches.

b. Tamper resistant fasteners manufactured by the McGard Company shall be used. It shall not be possible to enter the unit or remove any component without a special computer designed bit-wrench designed for this purpose. These bit-wrenches are supplied only by the manufacturer of the unit. All other types of fasteners shall not be acceptable due to the abundance of non-proprietary tools available for their removal.

c. The housing shall have an internal anchor baseplate that is fully welded to the cylinder two (2) inches above its base. The baseplate shall be fabricated with a minimum .50 inch thick A-36 grade steel plate, and shall have a four (4) inch diameter center hole for electrical conduit access, as well as three (3) oblong holes on a six (6) inch circular bolt pattern for anchor bolts. External mounting is not acceptable.

d. The unit shall have an access opening for anchor mounting and electrical wiring that is near the base of the bollard.

    1) The access opening shall have a cover plate flush with the unit, whose wall thickness and radius shall be the same as the bollard. The cover plate shall fit precisely into the oopening, have a weather resistant gasket to prevent water from entering the unit, and shall be held in place by two (2), one quarter (1/4) inch by one (1) inch countersunk, tamper resistant, proprietary fasteners as supplied by the manufacturer.

e. An opening shall be cut into the face of the housing at a point beginning 37.38 inches above its base, and continuing upward so that the opening is 12.38 inches high at its extreme rear surface, fourteen (14) inches high at the front, and 3.6 inches deep. The lowermost edge of the surface of the cut shall be sloped 25 degrees from the horizontal from rear to front. The upper edge of the opening shall be horizontal. The sides of the cutout shall be straight and parallel to one another, and the horizontal edges shall be perpendicular to the sides.

f. A plate of 7 gauge formed steel, with a center hole to accommodate the communications device, shall be fabricated to fit the opening in the housing. All edges of the plate and the center opening shall be straight in both planes.

g. The plate shall be seal welded to the housing so that the housing and plate appear to be one (1) piece. The weld shall be ground smooth and flush with the adjoining metal so that there are no visible separations or joints.

h. The housing shall be capped at the top with a three sixteenth (3/16) inch thick steel plate with a three (3) inch hole in the center. The plate shall be seal welded within the housing at the extreme upper edge. A lighting unit consisting of a combination blue strobe and beacon shall be mounted onto the plate.

4. Mounting

   a. The freestanding unit shall be mounted onto three bolts that are set in concrete. Standard three quarter (3/4) inch x twenty four (24) inch galvanized anchor bolts with galvanized nuts and washers shall be used. Unit shall mount one half inch above the concrete to allow air movement.

5. Electrical

   a. All electrical components shall have quick-disconnect terminals for easy service or removal. All wiring shall be concealed within the bollard and shall not be visible from the outside of the unit.
   b. The unit shall require 24 VAC and draw a maximum of 2.5 amperes under normal operation. The entire unit shall be surge protected.
   c. The speakerphone shall require 20 mA loop current at the unit. A 22 to 26 AWG gauge shielded twisted pair cable shall be used.

6. Lights

   a. Combination blue beacon and strobe: The unit shall have a combination lighting unit consisting of a strobe and beacon. The strobe shall generate 1,000,000 candlepower, and have a flash rate of no less than sixty (60) flashes per minute. The beacon, which serves as an area light, shall always be illuminated. A deep blue polycarbonate prismatic refractor that distributes the light in a horizontal pattern, making the flash bright and visible even at great distances, shall cover the strobe.
   b. Faceplate light: A long life, LED fixture shall be concealed within the unit above and directly forward of the communications device. This fixture will direct light onto the communications device faceplate, and shall be vandal resistant.

7. Communications

   a. The unit shall have a high quality, vandal resistant and ADA compliant speakerphone communications device.
   b. Standard Speakerphone: CB3100

      1) The speakerphone shall have one (1), one and one half (1.5) inch piezoelectric button labeled "PUSH FOR HELP," one (1), three eight (3/8) inch diameter red light emitting diode (LED) labeled "Call Being Placed," and one (1), three eight (3/8) diameter green LED labeled "Call Received." The speakerphone shall have an internally mounted electronics enclosure, auxiliary power, and shall be capable of playing up to two digitally stored voice messages upon activation. The electronics enclosure shall be capable of using interchangeable faceplates: a single-button faceplate, a two (2) button faceplate, or a two (2) button faceplate

with keypad. The speakerphone shall be programmable from a remote location and have a three number dialing capability. Battery backup shall be rated for sixteen (16) hours of active talk time and thirty two (32) hours of standby. Line powered phone devices, DIP switch programming, and push-to-talk devices are not acceptable.

2.25 CABLES

A. General Cable Requirements: Comply with requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security" and as recommended by system manufacturer for integration requirement.

B. PVC-Jacketed, TIA 232-F Cables:

1. Two pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, and individual aluminum-foil/polyester-tape shielded pairs with 100 percent shield coverage; PVC jacket.
2. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
3. NFPA 70, Type CM.
4. Flame Resistance: UL 1581 vertical tray.

C. PVC-Jacketed, TIA 485-A Cables: Two pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, PVC insulation, unshielded, PVC jacket, and NFPA 70, Type CMG.

D. Multiconductor, PVC, Reader and Wiegand Keypad Cables:

1. No. 22 AWG, paired and twisted multiple conductors, stranded (7x30) tinned copper conductors, semirigid PVC insulation, overall aluminum-foil/polyester-tape shield with 100 percent shield coverage, plus tinned copper braid shield with 65 % shield coverage, and PVC jacket.
2. NFPA 70, Type CMG.
3. Flame Resistance: UL 1581 vertical tray.
4. For TIA 232-F applications.

E. Paired, PVC, Reader and Wiegand Keypad Cables:

1. Three pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, individual aluminum-foil/polyester-tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 % shield coverage, and PVC jacket.
2. NFPA 70, Type CM.
3. Flame Resistance: UL 1581 vertical tray.

F. Paired, PVC, Reader and Wiegand Keypad Cables:

1. Three pairs, twisted, No. 20 AWG, stranded (7x28) tinned copper conductors, polyethylene (polyolefin) insulation, individual aluminum-foil/polyester-tape shielded pairs each with No. 22 AWG, stranded (19x34) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
2. NFPA 70, Type CM.
3. Flame Resistance: UL 1581 vertical tray.

G. Paired, Lock Cables:

1. One pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
2. NFPA 70, Type CMG.
3. Flame Resistance: UL 1581 vertical tray.

H. Paired, Lock Cables:

1. One pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
2. NFPA 70, Type CMG.
3. Flame Resistance: UL 1581 vertical tray.

I. Paired, Input Cables:

1. One pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, overall aluminum-foil/polyester-tape shield with No. 22 AWG, stranded (7x30) tinned copper drain wire, 100 % shield coverage, and PVC jacket.
2. NFPA 70, Type CMR.
3. Flame Resistance: UL 1666 riser flame test.

J. Paired, AC Transformer Cables:

1. One pair, twisted, No. 18 AWG, stranded (7x26) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
2. NFPA 70, Type CMG.

K. Elevator Travel Cables:

1. Steel center core with shielded, twisted pairs, No. 20 AWG conductor size.
2. Steel center core support shall be preformed, flexible, low-torsion, zinc-coated, steel wire rope; insulated with $60^0$C flame-resistant PVC and covered with a nylon or cotton braid.
3. Shielded pairs shall be insulated copper conductors; color-coded, insulated with $60^0$C flame-resistant PVC; each pair shielded with bare copper braid for 85 percent coverage.
4. Electrical grade, dry jute filler.

5. Helically wound synthetic fiber binder.
6. Rayon or cotton braid applied with 95 % coverage.
7. $60^0$C PVC jacket specifically compounded for flexibility and abrasion resistance; and complying with UL VW-1 and CSA FT1 flame rated.

L. LAN Cabling:

1. Comply with requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."
2. NFPA 262.

## 2.26 TRANSFORMERS

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

## 2.27 CABLE AND ASSET MANAGEMENT SOFTWARE

A. Computer-based cable and asset management system, with fully integrated database and graphic capabilities, complying with requirements in TIA/EIA 606-A.

1. Document physical characteristics by recording the network, asset, user, TIA/EIA details, device configurations, and exact connections between equipment and cabling.

a. Manage the physical layer of security system.
b. List device configurations.
c. List and display circuit connections.
d. Record firestopping data.
e. Record grounding and bonding connections and test data.

2. Information shall be presented in database view, schematic plans, or technical drawings.

a. Microsoft Visio Technical Drawing shall be used as drawing and schematic plans software. Drawing symbols, system layout, and design shall comply with SIA/IAPSC AG-01.

3. System shall interface with the following testing and recording devices:

a. Direct-upload tests from circuit testing instrument into the PC.
b. Direct-download circuit labeling into labeling printer.

B. Software shall be designed of the same version as security access system's central station and workstations and shall be installed on the designated PC, using a hard drive dedicated only to this management function. Hard-drive capacity shall be not less than 50 GB.

## 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.

### 3.2 PREPARATION

A. Comply with recommendations in SIA CP-01.

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

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

1. Record setup data for control station and workstations.
2. For each Location, record setup of controller features and access requirements.
3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
4. Set up groups, facility codes, linking, and list inputs and outputs for each controller.
5. Assign action message names and compose messages.
6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
7. Prepare and install alarm graphic maps.
8. Develop user-defined fields.
9. Develop screen layout formats.
10. Propose setups for guard tours and key control.
11. Discuss badge layout options; design badges.
12. Complete system diagnostics and operation verification.

13. Prepare a specific plan for system testing, startup, and demonstration.
14. Develop acceptance test concept and, on approval, develop specifics of the test.
15. Develop cable and asset-management system details; input data from construction documents. Include system schematics and Visio Technical Drawings in electronic format.

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

E. Coordinate layout and installation of Access Control Systems equipment with Owner's security representative.

1. Meet jointly with Owner to exchange information and agree on details of equipment arrangements and installation interfaces.
2. Record agreements reached in meetings and distribute them to other participants.

F. Coordinate layout and installation of the Access Control Systems cable pathways with telecommunications contractor.

## 3.3 CABLING

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

B. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.

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

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

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

## 3.4 CABLE APPLICATION

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

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

C. TIA 232-F Cabling: Install at a maximum distance of fifty (50) feet.

D. TIA 485-A Cabling: Install at a maximum distance of four thousand (4,000) feet.

E. 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 two hundred fifty (250) feet, and install No. 20 AWG wire if maximum distance is five hundred (500) feet.
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.

F. Install minimum No. 16 AWG cable from controller to electrically powered locks. Do not exceed two hundred fifty (250) feet.

G. Install minimum No. 18 AWG ac power wire from transformer to controller, with a maximum distance of twenty five (25) feet.

## 3.5 GROUNDING

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

## 3.6 INSTALLATION

A. Push Buttons: Where multiple push buttons are housed within a single switch enclosure, they shall be stacked vertically with each push-button switch labeled with one quarter (1/4) inch- high text and symbols as required. 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.

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

C. All electric locking and panic, and power transfer hardware will be supplied and installed by others. It is the security contractor's responsibility to provide power and interface the security system to the electric hardware.

## 3.7 CODE BLUE PHONE INSTALLATION

A. Provide as shown on TA series contract drawing.

B. Install as per manufactures instructions.

C. Coordinate the installation of Code Blue units with the owner.

D. Deliver equipment to the site and install in final location.

E. Using Owner-supplied parameters properly configure equipment.

F. Test equipment in accordance with the approved test plan, and provide written/electronic evidence of satisfactory completion of the testing.

## 3.8 WIRING FIRESTOPPING

A. Comply with requirements in Division 07 Section "Firestopping."

B. Comply with TIA/EIA-569-A, Annex A, "Firestopping."

## 3.9 IDENTIFICATION

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

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.

C. Label each terminal strip and screw terminal in each cabinet, rack, or panel.

1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the particular device as shown.
2. Each wire connected to building-mounted devices is not required to be numbered at the device if the color of the wire is consistent with the associated wire connected and numbered within the panel or cabinet.

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

## 3.10 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. The software developer shall be a Microsoft Gold Certified Partner.

## 3.11 FIELD QUALITY CONTROL

A. Perform tests and inspections.

B. Tests and Inspections:

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-B.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.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.

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

D. Prepare test and inspection reports.

## 3.12 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.

## 3.13 PROTECTION

A. Maintain strict security during the installation of equipment and software. Rooms housing the control station, and workstations that have been powered up shall be locked and secured with an activated burglar alarm and access-control system reporting to a central station complying with UL 1610, "Central-Station Burglar-Alarm Units," during periods when a qualified operator in the employ of Contractor is not present.

## 3.14 DEMONSTRATION

A. Train Owner's maintenance personnel to adjust, operate, and maintain security access system. See Division 01 Section "Demonstration and Training."

B. Develop separate training modules for the following:

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

5. Corporate management.

END OF SECTION 281300