SECTION 281300 – Access Control

1. **GENERAL**
   1. **SUMMARY**
      1. The system shall consist of access-control software that enables communication between computers with Windows 7 and higher operating systems and microprocessor-equipped smart controllers with distributed databases. The smart controllers make access-control decisions at doors, exits, entrances, etc., and communicate to PCs for programming instructions, event monitoring and record keeping. The controller(s) shall be designed specifically for access-control system applications.
      2. The controller(s) shall receive data input from other hardware components of the system, such as readers and relays. All system controllers shall be connected to the system server(s) where event history, cardholder data and system programming data shall reside. The controller(s) shall receive data input from, and provide system data to, the controlling system server(s).
      3. This performance specification provides the minimum requirements for the Access-Control system. The system shall include, but not be limited to, all equipment, materials, labor, documentation and services necessary to furnish and install a complete and operational system to include, but not be limited to, the following functions and components:
         1. Enabling valid access and preventing unauthorized access at facility portals
         2. Enabling alarm/alert notification of access breaches at facility portals and other points as desired
         3. Enabling data collection and management for a cardholder database at the facility
         4. The minimum requirements for controllers and I/O boards constituting interfaces for the Access-Control system
   2. **SECTION INCLUDES**
      1. Access-control software
      2. Access-control hardware, including microprocessor-equipped controllers and input/output boards
   3. **RELATED REQUIREMENTS**
      1. No interpretations of the meaning of the bid documents will be orally made to any bidder. Each request for such interpretation shall be made in writing.
      2. All work and materials shall conform to all applicable Federal, State, local and/or municipal codes and regulations governing the installation. If there is a conflict between this specification and the referenced standards, federal, state, local and/or municipal codes, it is the bidder's responsibility to immediately bring the conflict to the attention of the Engineer for resolution.
      3. The controllers, reader boards and input/output boards proposed in this specification shall be compliant with UL 294. The supplier shall be responsible for filing of all documents, paying all fees (including, but not limited to plan checking and permit) and securing all permits, inspections and approvals. Upon receipt of approved drawings from the authority having jurisdiction, the supplier shall immediately forward two sets of drawings to the Owner. These drawings shall either be stamped "Approved" or a copy of the letter stating approval shall be included.
      4. All controllers and connected boards, readers and the like shall be tested to ensure that a fully functioning system is designed and installed. The system supplied under this specification shall be a microprocessor-based system. The system shall utilize independently addressed, microprocessor-based controllers as described in this specification.
      5. Drawings and conditions of the project, including but not limited to General Conditions apply to work of this section.
   4. **ALTERNATES**
      1. Strict conformance to this specification is required to ensure that the installed and programmed system will function as designed, and will accommodate the future requirements and operations of the building owner. All specified operational features must be met without exception.
      2. The authorized representative of the manufacturer of the major equipment shall be responsible for the satisfactory installation of the complete system.
      3. All equipment and components shall be the manufacturer's current models. The authorized representative of the manufacturer of the major equipment, such as controllers, shall be responsible for the satisfactory installation of the complete system.
      4. All controllers and connected boards, readers and the like shall be tested to ensure that the system operates as specified. The system shall utilize independently addressed, microprocessor-based controllers as described in this specification.
      5. All equipment and components shall be installed in strict compliance with the manufacturer's recommendations.
      6. The equipment to be supplied will be considered only if it meets all sections of the performance specification. Any deviations of system performance outlined in this specification will only be considered when the following requirements have been met:
         1. A complete description of proposed alternate system performance methods with three (3) copies of working drawings thereof for approval by the Engineer, not less than ten (10) calendar days prior to the scheduled date for submission of bids.
         2. The supplier shall furnish evidence that the proposed or alternate system performance is equal or superior to the system operation stated in the specification. Such evidence shall be submitted to and accepted by the Owner, not less than ten (10) calendar days prior to the scheduled date for submission of bids.
         3. The supplier shall submit a point-by-point statement of compliance for all sections in this specification. The statement of compliance shall consist of a list of all paragraphs within these sections. Where the proposed system complies fully with the paragraph as written, placing the word "comply" opposite the paragraph number shall indicate such. Where the proposed system does not comply with the paragraph as written and the supplier feels the proposed system will accomplish the intent of the paragraph, a full description of the function as well as a full narrative description of how its proposal will meet its intent shall be provided. Any submission that does not include a point-by-point statement of compliance as described herein shall be disqualified. Where a full description is not provided, it shall be assumed that the proposed system does not comply.
      7. The acceptability of any alternate proposed system shall be the sole decision of the Owner or his authorized representative.
   5. **REFERENCES**
      1. Abbreviations and Acronyms
         1. UL® or ULI: Underwriters Laboratories, Inc
         2. ADA: Americans with Disabilities Act
         3. AFF: Above Finished Floor
         4. AHJ: Authority Having Jurisdiction
      2. Definitions
         1. Approved: Unless otherwise stated, materials, equipment or submittals approved by the Authority or AHJ.
         2. User: An administrator or operator who performs functions in the system in accordance with his/her system permissions and roles, unless otherwise stated.
      3. Reference Standards
         1. The equipment shall comply with the current provisions of the following codes and standards:
            1. UL 294 - Standard for Access Control System Units
            2. Factory Mutual (FM) approval
            3. Louisiana State Fire Marshal
            4. Americans with Disabilities Act (ADA)
            5. ISO-9000
   6. **SUBMITTALS**
      1. The contractor shall purchase no equipment for the system specified herein until the owner has approved the project submittals in their entirety and has returned them to the contractor. It is the responsibility of the contractor to meet the entire intent and functional performance detailed in these specifications. Approved submittals shall only allow the contractor to proceed with the installation and shall not be construed to mean that the contractor has satisfied the requirements of these specifications.
      2. Each submittal shall include a cover letter providing a list of each variation that the submittal may have from the requirements of the contract documents. In addition the contractor shall provide specific notation on each shop drawing, sample, catalog cut, data sheet, installation manual, etc. submitted for review and approval, of each such variation.
   7. **PRODUCT DATA**
      1. Data sheets shall be provided with the printed logo or trademark of the manufacturer for all equipment. Indicated in the documentation shall be the type, size, rating, style, and catalog number for all items proposed to meet the system performance detailed in this specification. The proposed equipment shall be subject to the approval of the Architect/Engineer.
   8. **CLOSEOUT SUBMITTALS**
      1. Two (2) copies of the following documents shall be delivered to the building owner's representative at the time of system acceptance. The closeout submittals shall include:
         1. Project-specific operating manuals covering the installed Access-Control System. A generic or typical owner's instruction and operation manual shall not be acceptable to fulfill this requirement.
         2. The application program listing for the system as installed at the time of acceptance by the building owner and/or local AHJ (disk, hard copy printout, and all required passwords).
         3. Name, address and telephone of the authorized factory representative.
   9. **MAINTENANCE MATERIALS SUBMITTALS**
      1. Spare Parts: The Contractor shall supply the following spare parts:
         1. Controllers - Two (2) percent of the installed quantity.
         2. I/O Boards - Two (2) percent of the installed quantity.
         3. Readers - Two (2) percent of the installed quantity of each type.
   10. **QUALITY ASSURANCE**
       1. All equipment and components shall be installed in strict compliance with each manufacturer's recommendations. Consult the manufacturer's installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the manufacturer's riser/connection diagram and details for all specific system installation/termination/wiring data.
       2. The engineered systems distributor must be licensed in the state of Louisiana and have been incorporated in the business in that state for a minimum of 3 years.
   11. **QUALIFICATIONS**
       1. The contractor shall have successfully installed similar access-control systems on a previous project of comparable size and complexity. The owner reserves the right to reject any control components for which evidence of a successful prior installation performed by the contractor cannot be provided.
       2. The contractor shall have in-house engineering and project management capability consistent with the requirements of this project. Qualified and approved representatives of the system manufacturer shall perform the detailed engineering design of central and remote-control equipment. Qualified and approved representatives of the system manufacturer shall produce all controller and equipment drawings and submittals, as well as operating manuals. The contractor is responsible for retaining qualified and approved representative(s) of those system manufacturers specified for detailed system design and documentation, coordination of system installation requirements, and final system testing and commissioning in accordance with these specifications.
   12. **FIELD CONDITIONS**
       1. It shall be the Contractor's responsibility to inspect the job site and become familiar with the conditions under which the work will be performed. Inspection of the building may be made by appointment with the Owner. Contractors are requested to inspect the building prior to the pre-bid meeting.
       2. The Contractor shall be responsible for prior coordination of all work and demolition with the Owner.
   13. **WARRANTY**
       1. The contractor shall warranty all materials, installation and workmanship for one (1) year from date of acceptance. A copy of the manufacturer's warranty shall be provided with closeout documentation and included with the operation and installation manuals.
       2. The System Supplier shall maintain a service organization with adequate spare parts stock within 50 miles of the installation. Any defects that render the system inoperative shall be repaired within 24 hours of the owner notifying the contractor.
2. **– PRODUCTS**
   1. **COMPONENTS**
      1. Manufacturers
         1. The manufacturer named herein shall be regularly involved in the design, manufacture or distribution of products specified in this document. The manufacturer's processes shall be monitored under a quality assurance program that meets ISO 9000 requirements.
         2. All products shall be listed by the manufacturer for their intended purpose.
         3. Products manufactured or distributed by IDenticard Systems Worldwide shall constitute the minimum type and quality of equipment to be installed.
         4. The specified PC-based Access Control and Monitoring Software shall be IDenticard® PremiSys by IDenticard Systems.
         5. All equipment and components shall be the manufacturer's current model. The authorized representative of the manufacturer of the major equipment shall be responsible for the satisfactory installation of the complete system.
         6. The contractor shall provide, from the acceptable manufacturer's current product lines, equipment and components that comply with the requirements of these specifications. Equipment or components that do not provide the performance and features required by these specifications are not acceptable, regardless of manufacturer.
      2. Computer and OS
         1. The system shall use a server computer that communicates with a client computer or computers. It shall be possible to install the system software so that one computer functions as server and client.
         2. The system uses an IDenticard Windows Service, Database Service and components requiring Internet Information System (IIS). It shall be possible to install the IDenticard Windows Service, Database Service and the components requiring IIS on the same or separate computers within a network.
         3. The system server computer shall have a 1.8 GHz (minimum), 2.1 (recommended) or faster processor (Intel® Core 2 Quad or equivalent or higher (recommended) or Intel® Core 2 Duo or equivalent (minimum) ), a minimum of 1536 MB or 2 GB (recommended) of RAM, 1 GB of free space on the hard drive for the PremiSys software, plus space for data; a CD-ROM drive or DVD drive; a 1024 x 768 24-bit video card; and a 10/100Base-T network interface card. The server computer shall have available as well COM ports if needed for the connection of system controllers using serial communications or for connection to third-party devices as described elsewhere in this specification. Any system client computer shall have a 1 GHz or faster processor (Intel Pentium® 4 processor or higher (or equivalent), a minimum of 1024 MB of RAM, 650 MB of free space on the hard drive for the PremiSys software, plus space for data; a CD-ROM drive or DVD drive; a 1024 x 768 24-bit video card; and at least two USB 2.0 ports for camera and printer.
         4. The recommended 32-bit operating system software for servers with all components installed shall be Microsoft® Windows Server® 2008 (R1 or R2);Microsoft® Windows® 7 Professional; or Microsoft® Windows Server® 2003. The minimum 32-bit operating system software for servers with all components installed shall be Microsoft® Windows Server® 2003. The minimum 32-bit operating systems for clients shall be; Microsoft® Windows® 7 Professional or higher; Microsoft® Windows Vista® Business or higher; or Microsoft Windows® XP Professional with Windows® Service Pack 2 or higher. The computer on which the components requiring IIS are installed shall have the Internet Information System (IIS) installed and enabled. All clients and servers in the system shall have Microsoft® Internet Explorer® 7 and Windows® Media Player.
         5. The system shall be compatible with all 64-bit Windows® operating systems, except 64-bit Windows XP®.
         6. Additionally, the database installed with the access-control software of this specification shall be Microsoft® SQL Server® 2008 Express R2. If the operating system is 32-bit, the 32-bit version of SQL Server shall be installed; if the operating system is 64-bit, the 64-bit version of SQL Server shall be installed.
         7. The system shall be of true multiuser design and capable of simultaneous operations from multiple client interfaces. A user logged onto any one client interface shall not affect the system control by users logged onto other client interfaces.
         8. Installation and Licensing
            1. The software installation application shall allow the user/installer to install the product for the first time or install a software upgrade, when new versions of the software are made available. The installation process for these two scenarios shall not vary significantly.
            2. The complete software with all components and features shall be installable at one time on one computer, using a full-installation option, by which this one computer becomes a client-server computer. This arrangement shall permit the installation of stand-alone systems. The software installation program shall also offer a client-only option to install remote clients on separate PCs.
            3. In addition, the software installation application shall offer to the user installation options to accommodate multiple server configurations. Specifically, the user shall be able to independently install  
               a) the system’s controlling service  
               b) the system’s database service  
               c) the components the system uses in conjunction with Windows® IIS.  
               In this way, user shall be able to install these constituents of the complete application on existing, separate servers to accommodate installation sites where, for example, a separate SQL database server already exists, a separate application server is needed and a separate IIS server already exists. The installation application shall be equally capable of allowing two of items a), b) and c) above in any combination, or all three, to be installed on one computer.
            4. Licenses shall be activated separately from the software installation.
            5. The software shall provide an automatic upgrade alert whereby users attempting to upgrade client stations before the server is upgraded are notified that the server must be upgraded first. An upgrade function shall also be provided that automatically flags users when they log into a client that is running a version of the software older than that on the server. The server shall then be capable of automatically “pushing down” the client software to the client and installing the upgrade on the client.
         9. Communications: Host
            1. The system controllers shall confirm receipt of all commands from the PC to ensure that no system transactions are lost.
            2. The communications between the host and connected controllers shall be continuously monitored with the host initiating all message exchange sequences. Supervision of system input points shall be provided by the controller. Failure or fault of data connections between the controller(s) and server(s) shall be indicated on the system display on a User Interface PC.
            3. It shall be possible in the system to require controllers to confirm with the host computer and its cardholder database that a card presented is a valid card. The host shall respond with a command either to confirm that access should be granted or to deny access, based on information in the cardholder database resident in the host. If this option is not enabled, the normal action of the card presentation being verified against the database on the controller shall be in effect. If this option is implemented in a system, users shall be able to define a timeout value, that is, a length of time that controllers shall wait for the host to respond. If the host does not respond within this set time, the controller shall function normally to either grant access or to deny it.
            4. It shall be possible to easily update firmware files on any controller and/or reboot the processor in any controller via software commands from the host.
         10. System Security and User Rights
             1. For each application-level user of the system, it shall be possible for the administrator to define the user name, enter the full first and last names of the user, define a password, and enter an e-mail address. It shall also be possible to establish activation and expiration dates for the user account in the system. Passwords permissible for use in the software shall conform to default Windows®-based requirements.
             2. The software shall include a system-administration application that allows administrators to manage operator accounts. Administrators shall be able to create groups having specific assigned rights and then to add operators to these groups and manage these groups. The administrators may edit any settings regarding an operator, in accordance with their own administrative rights within the system.
             3. The software shall enable administrators to assign time periods to users, which determine the days and times during which group rights are valid. Time periods can be associated with groups or users. Operators shall be able and need to enter a unique name as part of the definition of any time period.
             4. The software shall provide a method to limit the cardholder records a user may view and modify, in accordance with other system permissions. This method, termed cardholder filtering, allows the security administrator to create criteria to filter cardholder records and then assign the cardholder filter to groups of users so that only the records that meet the criteria are displayed for the logged-in users. If no such filter is assigned to a group of users those users shall be able to view all cardholders in the system unless the user belongs to another group that is assigned a cardholder filter. The software shall also provide a means by which users in a group can always see all cardholders; cardholder filtering shall not apply to them.
             5. The software shall provide a means to limit the hardware and other system objects that can be accessed in the software by users. This method, termed hardware filtering or permissions, allows the security administrator to “Allow” or “Deny” groups of users specific rights to Add or Edit, View, Delete, or perform Actions on the system objects. If a user belongs to more than one group and one group is denied permission, the Deny permission takes precedence. A user can be allowed or denied any or all of these permissions in any combination to result in the filtering deemed necessary by the security administrator. Systems incapable of filtering hardware from specific users’ ability to view, add, edit, delete or perform actions shall be deemed unacceptable.
         11. User Interface
             1. The User Interface shall incorporate a menu bar with drop-down menus and display icons for full system setup and operation. This menu and these icons shall offer to system users complete access on one screen to all system functions and system setup parameters to which the users have rights.
             2. Users shall be able to design, store and display multiple, individually created screens used to display cardholder information and data. The system shall support an unlimited number of user-defined screen layouts that shall accommodate the data fields in the system. The system shall additionally be built and delivered with a standard, ready-to-use data-entry screen. This product-standard screen shall be able to be modified and saved under a new screen name by the user.
             3. A data-entry screen shall be assignable to a system user for automatic display when that user logs in. It shall be possible to define default screens that always appear when a particular user logs onto the system. The system software shall allow an authorized user to select an appropriate screen layout from a menu on a per-client interface basis.
             4. The user interface shall provide windows and other controls for viewing system cardholder activity; monitoring and acknowledging alarms; and monitoring and controlling input points, relays and door configurations.
         12. Access Control Cards
             1. The system shall allow data to be entered to stipulate dates for the following parameters: card-activation dates, card-deactivation dates, vacation-start dates and vacation-end dates.
             2. It shall be possible in the software to designate a cardholder as exempt from area tracking for antipassback purposes. In addition, cardholders' records can include settings that allow them to benefit from extended time at doors and readers as specified under the Americans with Disabilities Act (ADA).
             3. The system shall allow a user to copy a cardholder’s card settings to create an additional card for that cardholder. All card settings other than the card number are copied to the additional card.
             4. The system shall allow a user to reassign a cardholder’s card settings to create a new card for that cardholder. All card settings other than the card number are copied to the new card.
             5. The system shall provide the means to assign multiple access control cards to a single cardholder record so that the user is not required to enter duplicate cardholder information for each card.
         13. Card Formats
             1. Users shall be able to select ABA and Wiegand reader card formats. Up to eight card formats shall be selectable per reader. The software shall accommodate multiple formats to allow the use of badges with different facility codes or different data lengths. These card data formatting capabilities shall allow the use of different reader technologies without modification to the software. The system shall support readers (with or without keypads) using magnetic-stripe, proximity, smart-card and biometric technologies.
             2. The software shall allow the configuration of multiple card formats to allow the use of badges with different site/facility codes and/or different data lengths. The maximum value for a facility code shall be 32 bits.
             3. The system shall support the use of cards with Wiegand or ABA formats, to accommodate magnetic-stripe, bar-code, smart-card, proximity and other cards.
             4. The software shall work with a unique identifier block on the identification card that contains a cardholder ID of up to 19 digits (64 bits), an optional issue code to uniquely identify lost and reissued cards and an optional PIN of up to 15 digits.
         14. Configuring Hardware
             1. Through the software application, users shall be able to view the firmware version numbers of any controller in the system.
             2. Through the software application, it shall be possible to view the total amount of memory installed in any controller as well as the amount of free memory available for use.
             3. The system shall support the connection of a virtually unlimited number of controllers when connecting controllers using Ethernet. When connecting via Ethernet the only limits are those imposed by the user’s PC memory and speed, network bandwidth and/or IP addresses available for use on the user’s network.
         15. Online Manual
             1. Selectable from the main menu of the software shall be a printable portable document file containing detailed instructions and background on the setup and operation of the system hardware components and a context-sensitiveHelp manual.
      3. PoE One-Door Reader Board
         1. The PoE One-Door Reader board shall be connected to a system controller and act as an interface between this controller and any of a variety of readers that can read ABA-formatted data or Wiegand®-formatted data from smart cards, proximity cards, magnetic-stripe cards, bar-coded cards or cards possessing a combination of these technologies. The board shall also be capable of supporting tri-stated LED control and buzzer control.
         2. The PoE One-Door Reader board shall support two (2) reading devices, the type being selectable through the application software. These reading devices are intended to control one door.
         3. The PoE One-Door Reader board shall use quick-disconnect terminal blocks for all interconnections to the interface. The PoE One-Door Reader board shall be intended for use in low voltage, Class 2 circuits only.
         4. The PoE One-Door Reader board shall communicate to a controller via Category 5 Ethernet cable, through a network interface. It shall be possible to connect up to 32 PoE One-Door Reader boards to a single IP Controller described in this specification, or to a single Two-Reader Controller described in the specification. All communications lines shall be supervised in the system, and transactions shall be provided in the system to alert the operator of offline or disconnect statuses. Communications to the controller shall be encrypted.
         5. Each PoE One-Door Reader board shall be uniquely addressable by the user through a range of IP addresses reserved on the controller containing the PoE One-Door Reader Board. The PoE One-Door Reader Board’s MAC address is used by the controller to link the board to the IP address.
         6. All PoE One-Door Reader boards shall be mounted in a three-gang junction box with an optional magnetic tamper switch.
         7. The PoE One-Door Reader board shall provide four (4) supervised inputs for use as a door-position input, a request-to-exit input and a tamper input. The states of the inputs shall be as follows: normally open; normally closed; 1 K normal, 2 K active; and 2 K normal, 1 K active. It additionally shall be possible to set the debounce and hold times for each input on the board. It shall be possible to set all input configuration via the system software.
         8. Held-open times – the time during which a door may be held open without generating a system alarm – for inputs on the board assigned as door-position points shall be software-selectable in two-second increments between 2 and 65,534 seconds.
         9. The first three (3) input points shall have a corresponding LED on the board that indicates the state of the point.
         10. The PoE One-Door Reader board shall also provide two Form-C, noninductive relay outputs for door-lock control or alarm signaling. Control of the relays shall be software-assignable to be triggered by card presentations, time zones and/or other system actions. The contact ratings shall be 5 A at 28 VDC. The relays shall be configurable for normal (relay energized when “on”) or inverted (relay de-energized when “on”) action. Pulse time of a relay used as a door-lock relay shall be software-selectable between 1 and 255 seconds.
         11. It shall be possible via the system software to link an input or relay on the PoE One-Door Reader board to cause an action on any other relay on the same board or on any other board wired to the same controller and to select the action that a linked relay will take when the triggering input or relay is activated.
         12. The PoE One-Door Reader board shall also provide a jumper-like input for optional use to indicate tamper status.
         13. The PoE One-Door Reader board shall allow the board to be powered over the Ethernet connection or via a separate 12-VDC power supply to the board. The input power shall be passed through to the reader terminal block (port) and shall be available for powering a reader.
3. **– EXECUTION**
   1. **PREPARATION**
      1. The Contractor shall order all required parts and equipment upon notification of award of the work.
      2. The Contractor shall bench test all equipment prior to delivery to the job site.
      3. The Contractor shall verify the availability of power where required. If a new source of power is required, a licensed electrician shall be used to install it.
      4. The Contractor shall arrange to obtain all programming information including access times, free access times, doors, operator levels, etc.
   2. **INSTALLATION**
      1. General
         1. The Contractor shall coordinate with the telecommunications contractor for interface with their LAN system.
         2. The Contractor shall carefully follow the instructions in the manufacturers' Installation Manual to insure all steps have been taken to provide a reliable, easy to operate system.
         3. The Contractor shall coordinate with the Architectural Hardware Consultant to interface with all electric locks.
         4. The Contractor shall perform all work as indicated in the drawings and specifications.
         5. The Contractor shall install the appropriate cable from the controllers to readers, door contacts, request-to-exit devices, and electric locks at each door.
         6. All communications cables shall be kept away from power circuits.
         7. The Contractor shall also execute adequate testing of the system to ensure proper operation.
      2. Conductors and Raceway
         1. The entire system shall be installed in a skillful manner in accordance with approved manufacturer's installation manuals, shop drawings and wiring diagrams. The contractor shall furnish all, wiring, cabinets, enclosures and similar devices necessary for the complete installation. All wiring shall be of the type required by the NEC and approved by local authorities having jurisdiction for the purpose.
         2. Any shorts, opens, or grounds found on new or existing wiring shall be corrected prior to the connection of these wires to any panel, component or field device.
         3. The contractor shall neatly tie-wrap all field-wiring conductors in the spaces provided in the controller-panel enclosures and secure the wiring away from all circuit boards and control equipment components. All field-wiring circuits shall be neatly and legibly labeled in the controller as needed. No wiring splices shall be permitted in a controller enclosure. There shall be no components mounted in any PremiSys enclosure other than those specified by the manufacturer.
      3. Test & Inspection
         1. All wiring shall be tested for continuity, shorts and grounds before the system is activated.
         2. All test equipment, instruments, tools and labor required to conduct the tests shall be made available by the installing contractor.
         3. The system, including all its sequence of operations, shall be demonstrated to the Owner or his representative. In the event the system does not operate properly, the test shall be terminated. Corrections shall be made, and the testing procedure shall be repeated until it is acceptable to the Owner or his representatives.
         4. At the final test and inspection, a factory-trained representative of the system manufacturer shall demonstrate that the system functions properly in accordance with these specifications. The representative shall provide technical supervision, and shall participate during all of the testing for the system.
         5. A letter from the Contractor shall be provided to certify that the system is installed entirely in accordance with the system manufacturer's recommendations and within the limitations of the required listings and approvals, that all system hardware and software has been visually inspected and functionally tested by a manufacturer's certified representative, and that the system is in proper working order.
      4. Training
         1. The System Supplier shall schedule and present a minimum of two (2) hours of documented, formalized instruction for the building owner, detailing the proper operation of the installed System.
         2. The instruction shall be presented in an organized and professional manner by a person factory-trained in the operation and maintenance of the equipment and who is also thoroughly familiar with the installation.