USF UNIVERSITY OF SOUTH FLORIDA

# DESIGN & CONSTRUCTION GUIDELINES

# APPENDIX E
# ACCESS CONTROLS SYSTEM DESIGN GUIDELINES
## (TAMPA CAMPUS)

EDITION: **FEBRUARY 18, 2021**
**USF FACILITIES MANAGEMENT - OPERATIONS**

# APPENDIX E – ACCESS CONTROL SYSTEM

**INDEX** **SECTIONS** **TITLE** **FEBRUARY 18, 2021**



## PART 1 GENERAL

### 1.1 SCOPE OF WORK

**A.** The scope of the work included under this division of the Specifications shall include installing a card access system for managing access to buildings. Specifically, this is accomplished by using card readers on the exterior doors of the various buildings. Additional access control may be required at Department Suites Doors and open use classrooms as determined by the user group and educational outreach. The USF ID card will be used for this system. This will require that all students, faculty, and staff who need after-hour access to have a valid USF ID card. All access control doors will be re-keyed with the University Police master key to increase the security. Building occupants will no longer carry exterior door keys.

**B. Definition:**

1. **Contractor:** In this section the Contractor refers to the Access Control Integrator.
1. **Owner/User:** In this section the Owner/User refers to USF.

### 1.2 ACCESS CONTROLS

**A.** Contractor is to provide and install Lenel Mercury products and ancillary products needed to fulfill the sequence of operation for each door as shown in the construction documents.

**B.** Contractor is to provide programming (points and alarms) and commissioning the system.

**C.** Installation, wiring and conduits from panel to the doors & all hardware tied into the access control system are done by this contractor (including 120 VAC).

**D.** It is the responsibility of this contractor to coordinate with USF Operational Technology for programming/configuration to properly integrate the door hardware with the access control system to deliver a fully functional system.

### 1.3 DESCRIPTION OF WORK

**A.** The Integrated Security Management System (ISMS) shall manage the security operations for a single site or for multiple sites. Installing the ISMS and bringing it to operational status requires the following major steps:

**1.** Coordinate with Operational Technology to determine operational requirements to comply with campus standards.
**2.** Install and configure, where necessary, the communications network providing communications between the Client and Server computer workstation.
**3.** Install and integrate Access Control, Alarm Monitoring, and related security hardware.
**4.** Configure local access panels and ISMS Server computer system to communicate with one another.
**5.** Coordinate with Operational Technology to test and confirm functionality after all components of the system have been installed and are communicating and operating properly.

## 1.4 SUBMITTALS

### A. Shop Drawings

**1.** Provide complete shop drawings which include the following:

**a.** Indicate all system device locations on architectural floor plans. No other system(s) shall be included on these plans.
**b.** Include full schematic wiring information on these drawings for all devices. Wiring information shall include cable type, conductor routings, quantities, and connection details at devices.
**c.** Include a complete access control system one line, block diagram.
**d.** Include a statement of the system sequence of operation.
**e.** The shop drawings have to be approved by the engineer of record and USF Facilities Management before any commencement of the work.

### B. Contract Close-Out Submittals

The USF Tampa access control system is fully integrated campus wide and familiar to the operational & maintenance technical team. Thus, unless specified otherwise by USF, the product data and owner training is not required.

**1.** Provide electronic files of manuals including operating instructions, maintenance recommendations, parts list, wiring & connection diagrams modified to reflect as-built conditions.
**2** Provide spare parts and attic stock as specified in the contract documents.

## 1.5 QUALITY ASSURANCE

**A.** The manufacturers of all hardware and software components employed in the system shall be established vendors to the access control/security monitoring industry for no less than five (5) years.

**B.** The security system integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems similar in size and scope to that outlined herein for a period of no less than five (5) years.

**C.** The security system integrator shall supply information attesting to the fact that their firm is an authorized product dealer for the system proposed.

**D.** The security system integrator shall supply information attesting to the fact that their installation and service technicians are competent factory trained personnel capable of maintaining the system and providing reasonable service time.

**E.** The security system integrator shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the security system integrator in the last five (5) years.

**F.** There shall be a local representative and factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for these systems. Local shall be defined as an area in a fifty (50) mile radius of installed location.

## PART 2 PRODUCTS

### 2.1 MANUFACTURERS

### 2.1.1 PRODUCTS

**A. Approved Field Hardware:**

LNL-3300 controller
LNL-4420 controller – elevator controls
LNL-1320 – Dual Reader board
LNL-1300 – Single Reader board
LNL1100 – Digital Input board
LNL-1200 – Digital output board

**B. Integrated Security Management System:**

Lenel Onguard 7.5 or latest version

### 2.1.2 CONTRACTORS

**A.** Any approved Lenel Partner:
(Installers: ADT, IFSS, SIEMENS, etc.).

### 2.2 MATERIALS

**A.** This Section covers the provision of an Integrated Security Management System (ISMS) for the University of South Florida Tampa campus including all items and subsystems shown on drawings or otherwise required by these Specifications for USF Building.

**B.** The requirements for these specifications shall be understood to be the USF Standard. The requirements shall be expanded as necessary to ensure quality. However, unless USF prior written approval is obtained, the requirement herein shall not be deleted or revised.

**C.** USF shall be hereinafter referred to in this document as the OWNER and the bid respondents shall be referred to as the SECURITY CONTRACTOR. The term OWNER includes direct employees and other appointed OWNER agents such as architects or consultants. These agents may be requested by the OWNER to represent the OWNER in undertaking certain project tasks.

**D.** If any statement in this or any other specification conflicts with any provision of the General Terms and Conditions of the contract, the provision stated in the General Terms and Conditions shall have precedence. Any questions that require additional interpretation and guidance shall be immediately brought to the OWNER'S attention.

### 2.2.1 SECTION INCLUDES

**A.** This section covers the provision of ISMS including all items and Subsystems shown on drawings or otherwise required by these specifications.

**1** ISMS Computer, Hardware, software, and control panels for access control and alarm management.
**2.** Card readers and other security input/output devices for access control and alarm monitoring of secured areas.
**3** Automatic Doors & operators:
**4** Video Surveillance System.

### 2.2.2 RELATED SECTIONS

**A** Conduit, Raceways and Cable trays: Division 27, Communications.

**B** Fire stopping Penetration through Rated Construction: Division 26, Electrical.

**C** Electrical, Cabling, and Wiring: Division 26, Electrical.

**D** Door Hardware: Division 8, Openings.

## 2.3 SYSTEM REQUIREMENTS

**A.** The vendors provide hardware installation that will integrate with the existing USF Tampa access control system

## 2.4 SOFTWARE

### 2.4.1 Host Server Software and Operator Workstation Software:

**A** USF Tampa campus operates a campus wide access control system software. All new equipment and system components must be fully integrated into the existing software.

### 2.4.2 Security Management Software:

**A** Existing Lenel Onguard 7.5 or latest version.

## 2.5 HARDWARE

**2.5.1 Host Server and Operator Workstations:** Existing server and workstations.

**2.5.2 Control Panels:** Lenel LNL-3300 and LNL-4420 for elevator control. The ISMS control panels shall be intelligent and fully stand-alone processor capable, making all local access control and alarm monitoring decisions without host server dependency. Control panels shall support and provide the following:

**A.** UL listed under UL 294 and UL 1076; FCC Part 15 and CE compliant.

**B.** RS232 and RS422 communications ports for cascading/clustering multiple control panels via a single communications port interface to ISMS hosting server or operator workstations.

**C.** Control panel cabinet shall be of an industrial grade enclosure with knockouts for field wiring and have a key-locked and tamper protected door.

**D.** Low voltage power supply with uninterruptible battery backup allowing continued operations for a minimum of two (2) hours at full load.

**2.5.3 Control Panel Interfaces:** The ISMS control panels shall support on board and/or expansion interface boards for access control readers, alarm monitoring, and input/output control. Control panels shall support and provide the following as required:

**A.** Access Control Reader Interfaces:

**1.** Shall support hard-wired connections to readers, including power and communications. Connections shall be supported at a minimum distance of two-thousand (2,000) feet (or 610 meters) utilizing 22 AWG 2-pair shielded and unshielded cabling.

**2.** Shall support supervision, monitoring, and processing of the following:

**a.** Reader tamper and communications.
**b.** Status changes from locally wired door sensor and request to exit device.

**3.** Shall support card only Multi-Technology Aptiq MTMS15-485 style readers of the following technologies:

**a.** Smart Card
**b.** Magnetic Stripe

**B. Access Control Card Readers:**

**1. Reader Technology:** As specified by selected card technology and application requirements; compatible with ISMS control panels and commercially available from industry leading manufactures that include but not limited to:

**a.** Aptiq MTMS15-485 (campus standard)

Note: Refer to Appendix C, Student Housing Design Guidelines for USF Housing access control requirement.

2. The specified card and reader manufacturer shall support a full product line that offers multiple models and/or styles to fit various installation and application requirements including:

   a. Card only.
   b. Rugged, weatherized enclosures rated for indoor and outdoor mounting.
   c. Rated for mounting on metal and non-metal surfaces.
   d. Provide audible and visual indicators for reader status and validation of granted and denied access.

3. Provide quantities for each model and/or style indicated on drawings.

**C. Electric Door Hardware:**

1. Electronic locking devices shall have a separate power supply to support the locks specified below. The unit shall incorporate integral battery charging capabilities and a fused line voltage input for a minimum of eight (8) individual locks. All power supplies shall be equipped with optional battery pack for up to forty-eight (48) hours. The unit shall be equipped with a module to accommodate fire alarm NC contacts when a fire alarm activates.
2. All locks shall be fail-secure unless otherwise specified by the Security Consultant/Designer. Locks specified, as being fail-safe shall be installed in accordance to Section 5-2.1.6.2 of NFPA Life Safety Code 101.
3. The SECURITY CONTRACTOR shall coordinate with Operational Technology for the interconnection of the specified ISMS.
4. Specified Products

   a. Electric Mortise Lock: Sargent 8271.
   b. Exit Device/Crash Bar: Von Duprin.
   c. Electric Strike:
      i. Sargent.
      ii. Von Duprin requires prior approval by Operational Technology for retrofit projects only. Not approved for new building projects.
   d. Magnetic Locks are not allowed on this cam us unless pre-approved in writing by the University Facilities Management Code Enforcement department.

5. Provide quantities for each model indicated on drawings.

**D. Door Hardware Configuration:**

1. Card access controlled doors shall be equipped with a passive infrared request-to-exit device specifically designed for electromechanical lock release. Device shall be equipped with a DPST (NO & NC) 1-amp contact.
2. Card access controlled doors shall be equipped with a non-illuminating emergency exit button to momentarily deactivate the magnetic lock. The device shall be equipped with DPDT contacts with one side sending a REX to the ISMS control panel and the other directly interrupting power to the magnetic lock. The device shall fit into a single gang electrical box.
3. Card access controlled doors shall be equipped with a touch sense exit device to momentarily deactivate the magnetic locking device. The device shall be 24 VDC and equipped with DPST (NC & NO) contacts.

**E. Intrusion Detection Devices:**

1. **Door Sensor Contacts:**
   a. Recessed magnetic door contacts shall be provided for all card access doors and doors requiring intrusion detection. Door contacts shall be provided on single doors and both leaves of double doors at locations indicated on drawings. Color to match existing finish.

**b.** Where building structure makes it impossible to install conduit within the wall or doorframe, the SECURITY CONTRACTOR shall substitute surface-mount contacts with armored cable for the specified contacts.
**c.** Heavy-duty door contacts with armored cable shall be provided for all Roll-Up Doors where indicated on the drawing.
**d.** All devices shall be wired point to point and to the nearest ISMS control panel interface.

**2. Motion Detectors:**
**a.** WALL MOUNTED or CEILING MOUNTED passive infrared (PIR) motion detectors shall be provided where indicated on drawings. Motion detectors shall be masked or oriented to minimize the likelihood of nuisance alarms caused by environmental conditions.
**b.** All devices shall be wired point to point and to the nearest ISMS control panel interface.
**c.** A 12 VDC centralized power supply shall be utilized to power motion detectors.

## PART 3 EXECUTION

### 3.1 SECURITY CONTRACTOR

**A.** The SECURITY CONTRACTOR shall be a local installation and service organization, currently as a factory authorized representative by the manufacturer of the specified system.

**B.** The SECURITY CONTRACTOR shall provide a minimum of three (3) references whose systems are of similar complexity and have installed and maintained by the SECURITY CONTRACTOR in the last five (5) years.

**C** At time of bid, the SECURITY CONTRACTOR shall be licensed by the state or local jurisdiction to perform security work within the state. Contractors who have security licenses or permits pending shall not be considered acceptable for bidding on this project.

**D.** The SECURITY CONTRACTOR shall assure that all personnel working on the project are registered with the state or local jurisdiction Systems Licensing Board as provided for by Current state statutes.

**E.** At the time of bid, the SECURITY CONTRACTOR shall provide satisfactory evidence of liability Insurance and Worker's Compensation coverage for employed personnel as required by law.

### 3.2 PROJECT MANAGEMENT

**A**. The SECURITY CONTRACTOR shall provide an on-site, factory-trained technician to assist, advice and mange installing personnel.

**B** All of the SECURITY CONTRACTOR'S personnel and operating forces Including subcontractors and delivery personnel, shall be made aware of, and shall comply at all times, with the regulations, project requirements, and directions of responsible OWNER personnel.

### 3.3 PERSONNEL

**A.** The SECURITY CONTRACTOR'S personnel shall be qualified to accomplish all work promptly and satisfactorily. The OWNER shall be advised in writing of all designated service and support personnel responsible for installation as well as pre- and post-warranty service.

**B** The SECURITY CONTRACTOR'S shall provide proof that designated service and support personnel have successfully completed the appropriate level of both hardware and software training offered by the manufacturer for installation and maintenance of the specified system.

**C.** STUDENT, STAFF AND FACULTY INTERACTION: All technicians must uphold the highest level of professionalism. USF is an environment where unprofessional conduct is not tolerated. All company employees shall be identifiable by their name and company apparel clearly visible at all times.

## 3.4 ACCESS CONTROL SYSTEM - INSTALLATION

**A General:** The contractor shall install all system components and appurtenances in accordance with the manufacturer's instructions, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation. Provide mounting hardware as required.

**B Installation:** All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code. Cable shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring.

**C. Device Wiring and Communication Circuit Surge Protection:** All inputs shall be protected against surges induced on device wiring. Outputs shall be protected against surges induced on control and device wiring installed outdoors and as shown. All communications equipment shall be protected against surges induced on any communications circuit. All cables and conductors, except fiber optics, which serve as communications circuits from security console to field equipment, and between field equipment, shall have surge protection circuits installed at each end.

**D**. All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code.

**E.** All wiring conductors connected to terminal strips shall be wired individually. Each cable or wiring group being extended from a panel or cabinet to a building mounted device shall be identified with the name and name of the particular device as identified and shown on building drawings.

**F.** All exposed wiring inside and outside the control console, cabinets, boxes, and similar enclosures, shall be dressed down neatly and secures with wiring cleats or wire ties.

**G.** All exposed metallic flexible conduit and armored cable shall be dressed down neatly and secured with low profile, metal fasteners.

**H.** All cabinets, boxes, and similar enclosures containing security system components and /or cabling and which are accessible to employees or to the public shall be provided with a lock. Boxes above ceiling level in occupied areas of building shall not be considered to be accessible.

**I.** All 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 tamper proof screws.

**J.** End -of-line resistors shall be installed at the field device location and not at the controller panel location.

**K.** System devices identified on building drawings are intended to generally indicate areas where such devices are to be located. Security Contractor shall be responsible for determining final location of these devices in accordance with OWNER'S requirements.

**L.** Riser diagrams are schematic and do not show every conduit, wire box, fitting, or other accessories. Provide such materials as necessary for a complete and functioning installation. Install in accordance with referenced codes and these specifications. Use weatherproof equipment or covers where installed in areas exposed to weather.

**M.** All control wiring shall be labeled at both ends and wire label shall be indicated in as-built drawing.

## 3.5 COMMISSIONING AND TRAINING

**A** Perform commissioning as specified in eth construction documents.

**B.** The USF Tampa access control system is fully integrated campus wide and familiar to the operational & maintenance technical team. Thus, unless specified otherwise by USF, the owner training is not required.

## 3.6 TESTING

**A. General:** The contractor shall perform pre-delivery testing, site testing, and adjustment of the completed ISMS. The contractor shall provide all personnel, equipment, instrumentation, and supplies necessary to perform all testing. Written notification of planned testing shall be given to the owner at least fourteen (14) days prior to the test and in no case shall notice be given until after the contractor has received written approval of the specific test procedures? Test procedures shall explain in detail, step-by-step actions and expected results demonstrating compliance with the requirements of the specification. Test reports shall be used to document results of the tests. Reports shall be delivered to the owner within seven (**7**) days after completion of each test. The test procedures are determined and written by the A/E.

**B. Performance Verification Test:** The contractor shall demonstrate that the completed ISMS complies with the contract requirements. Using approved test procedures, all physical and functional requirements of the project shall be demonstrated and shown.

**C.** The SECURITY CONTRACTOR is required to place entire system into full and proper operation as designed and specified.

1. Verify that all hardware components are installed properly, connected, communicating, and operating correctly.
2. Verify that all system software is installed, configured, and complies with specified functional requirements.

**D.** The SECURITY CONTRACTOR shall perform final acceptance testing in the presence of OWNER'S representative, executing a point by point inspection against a documented test plan that demonstrates compliance with system requirements as designed and specified.

1. Submit documented test plan to CM/A&E/OWNER at least fourteen (14) days in advance of acceptance test, Inspection and check-off.
2. Conduct final acceptance tests in presence of OWNER'S representative, verifying that each device point and sequence is operating correctly and properly reporting back to control panel and control center.
3. Acceptance by OWNER is contingent on successful completion of check-off; is check-off is not completed due to additional work required, re-scheduled and perform complete check-off until complete in one pass, unless portions of systems can be verified as not affected by additional work. Industry standard is for the architect to determine substantially complete, which includes beneficial occupancy
4. The System shall not be considered accepted until all acceptance test items have been successfully checked off. Beneficial use of part or all of the system shall not be considered as acceptance.

**E.** The SECURITY CONTRACTOR shall provide system operations, administration, and maintenance training by factory trained personnel qualified to instruct:

1. OWNER will designate personnel to be trained.
2. Provide printed training materials for each trainee including product manuals, course outline, workbook or student guides, and written examinations for certifications.
3. Provide hands on training with operational equipment.
4. Training shall be oriented to the specific system being installed under this contract as designed and specified.

## 3.7 WARRANTY, MAINTENANCE AND SERVICE

**A. Warranty:** The ISMS shall be warranted by the contractor for one (1) year from the date of final system acceptance/substantial completion.

**B. Maintenance and Service:** The contractor shall provide all services required and equipment necessary to maintain the entire ISMS in an operational state as specified for a period of one (1) year after formal written acceptance of the system, and shall provide all necessary material required for performing scheduled adjustments or other nonscheduled work.

**C Description of Work:** The adjustment and repair of ISMS includes computer equipment, software updates, signal transmission equipment, access control equipment, facility interfaces, and support equipment. Responsibility shall be limited to contractor installed equipment. Provide the manufacturers required adjustments and other work as necessary.

**D Personnel:** Service personnel shall be qualified to accomplish all work promptly and satisfactorily. Provide proof that Service personnel have successfully completed the appropriate level of both hardware and Software training offered by the system manufacturer. The owner shall be advised in writing of the name of the designated service representative and of any change in personnel.

**E Inspections:** The contractor shall perform two inspections at six (6) month intervals or more often if required by the manufacturers. This work shall be performed during regular working hours, Monday through Friday, excluding Federal holidays. These inspections shall include:

1. Visual checks and operational tests of the central processor, local processors, monitors, keyboards, system printers, peripheral equipment, ISMS equipment, power supplies, and electrical and mechanical controls.
2. Clean system equipment, including interior and exterior surfaces.
3. Perform diagnostics on all equipment.
4. Check and calibrate each ISMS device.
5. Run system software and correct diagnosed problems.
6. Resolve previous outstanding problems.

**F Emergency Service:** The owner shall initiate service calls when the ISMS is not functioning properly. Qualified personnel shall be available to provide service to the complete SMCS. The owner shall be furnished with the telephone number where the contractor's service supervisor can be reached at all times. Service personnel shall be at the site within four (4) hours after receiving a request for service. The ISMS shall be restored to proper operating condition after one (1) calendar day.

**G Software:** Existing USF software.