

Appendix 1 – LACCD Districtwide Security Performance Requirements

LACCD Districtwide Security Performance Requirements

SECTION LISTING

28 01 10	Overview
28 13 00	Access Control System
28 13 01	Access Control System Installation
28 13 26	Access Control Remote Devices

28 01 10 Overview

1. The operation and maintenance of the Physical Access Control System software, servers, and field processors fall under the authority of LACCD IS Department. Any and all changes or modifications to any of these shall be coordinated with the LACCD IS Department prior to commencement of activity.
2. The operation and maintenance of the Physical Access Control System electrified locks and associated door hardware fall under the authority of LACCD Facilities Department. Any and all changes or modifications to any of these shall be coordinated with the LACCD Facilities Department prior to commencement of activity.

28 13 00 Access Control System

1. DESCRIPTION

- a. The PACS componentry consists of items including, but not limited to:
 - Lenel-S2 System Controllers
 - Lenel-S2 Reader Interfaces
 - HID Card Readers
 - Lenel-S2 software client software
 - Lenel credential design and printing software
 - Districtwide Lenel-S2 Master Server
 - Distributed Lenel-S2 servers (1 at each College)
 - Lenel-S2 OnGuard Enterprise Software
 - Cabling and network supporting infrastructure and devices
- b. All servers and software associated with the PACS shall be administered by LACCD IS Department.
- c. LACCD shall retain a Master Lenel Integrator to oversee system programming, configuration, and commissioning alongside the Integrator selected to perform the installation and configuration of the field devices.
- d. Per LACCD Chancellors Directive 185, all perimeter doors into buildings containing classrooms as well as all perimeter doors leading directly into classrooms shall have electronic access control integrated into the Districtwide PACS.

28 13 01 Access Control System Installation

1. DESCRIPTION

- a. Refer to Appendix 2 – Typical Access Control Installation Details for installation of all components. Installation details shall be clarified, deleted, or added to on a project by

LACCD Districtwide Security Performance Requirements

project basis through coordination between the Designer, the General Contractor, if applicable, and the LACCD CPM.

- b. The Integrator for this scope shall be responsible for the procurement and installation of a complete Physical Access Control System, including:
 - all electronic components generally considered to be directly related to the functions of an access control system
 - integration of this system with the existing PACS
 - procurement and transfer of any and all applicable Lenel hardware, software, or firmware licenses.
- c. Based upon the scope requirements as detailed in 28 13 01.1.b above, the integrator shall have the following certifications:
 - Be designated by Lenel-S2 as a Value-Added Reseller (VAR)
 - Be established as, or obtain status as, an LACCD Lenel-S2 VAR
 - Have a Registered Communications Distribution Designer (RCDD) on staff
- d. Some of the PACS components will be specified and provided under Division 8 – Doors and Windows. This will typically include hardware attached to the door and power supplies for hardware attached to the door. Project designer shall add a matrix of responsibility to project drawings as to delineate scope responsibilities. Contractor shall coordinate all access control installation activities with Division 8 Contractor.

2. INSTALLER REQUIREMENTS

- a. All installation of materials and equipment specified under the LACCD Districtwide Security Performance Specifications shall be completed by Lenel Certified Technicians.
- b. At least one installer assigned to the project shall have a current Lenel Enterprise certification.

3. PROJECT MANAGEMENT

- a. Integrator shall provide a Project Manager who is experienced in the administration and supervision of the security field and electrical work, both within the various types of security integration and with relation to other types of work and who is hereby authorized to act on behalf of Integrator.
- b. The project manager responsibilities will include but are not limited to providing schedules, attending project meetings, submittals, safety, quality control, and testing, training and as-built documentation.
- c. The project manager must be an employee of Integrator and working in the security field.

4. PROJECT COORDINATION

LACCD Districtwide Security Performance Requirements

- a. Integrator shall coordinate meetings with all related trades to ensure that all necessary work by other trades is proceeding according to the project schedule and that there are no gaps in scope to provide a complete functioning access controlled door system.
- b. Related trades include but are not limited to the Door Hardware vendor, Auto-operator accessibility door vendor, LACCD Campus IT, Master Integrator, Low Voltage Contractor, and Electrical Contractor.

5. SYSTEM CONFIGURATION

- a. Integrator shall provide the necessary reader licenses to support the quantity of readers for the project. Licenses are ordered in blocks of 64 readers and the number of readers shall be rounded up to the nearest multiple of 64 to obtain the correct quantity of licenses.
- b. The licenses shall be delivered to the District representative to be added to the system license server.
- c. Integrator shall complete the programming sheets that document the panel loading schedule and provide to the LACCD PM so the Master Integrator can complete the programming in a timely manner prior to system power up and commissioning. Sample schedules and instructions will be provided by the LACCD PM.
- d. Integrator shall program the IP addresses according to the scheme provided by the LACCD PM and document them in the IP device worksheet along with MAC addresses and user names and passwords for all field hardware panels.
- e. Integrator shall install the access panels and interface boards according to the programming sheets completing all wiring between boards, lock control modules and field wiring.
- f. All locks shall be tested along with the door position switches and request to exit devices and deficiencies corrected prior to scheduling a system commissioning test with the LACCD PM and Master Integrator.

28 13 26 Access Control Remote Devices

1. APPROVED DEVICES

- a. Refer to Appendix 2 for all typical device installation and cabling details.
- b. The following is a list of access control field equipment that is approved for installation based upon system requirements:
 - I. Single Reader Interface Module: Lenel LNL-1300-S3
 - II. Dual Reader Interface Module: Lenel LNL-1320-S3
 - III. Intelligent Dual Reader Controller: Lenel LNL-2210
 - IV. Intelligent Dual Reader Controller: Lenel LNL-X2220
 - V. Advanced Dual Reader Controller: Lenel LNL-X4420
 - VI. Intelligent System Controller: Lenel LNL-X3300
 - VII. 16 Input Control Module: Lenel LNL-1100-S3
 - VIII. 16 Output Control Module: Lenel LNL-1200-S3
 - IX. RS-485 Multiplexer: Lenel LNL-8000
 - X. Standard Wall Mount Card Reader: HID iCLASS SE R40 using OSDP communication, Mobile ready 920NMPTEKEA007
 - XI. Wall Mount Card Reader with Integral Keypad: HID iCLASS SE RK40 using OSDP communication, Mobile ready 921NMPTEKEA008

LACCD Districtwide Security Performance Requirements

- XII. Mullion Mount Card Reader: HID iClass SE R15 using OSDP Communication, Mobile ready 910NMPTEKEA007
- XIII. Unified Power Enclosure with SNMP: LifeSafety FPO150-D8C8P2NL2E4M
- XIV. Unified Power Enclosure: LifeSafety FPO150-D8C8P2E4M
- XV. Request-to-exit device (when not integrated into locking hardware): Bosch DS160
- XVI. Door Position Switches: Schlage 7764

2. CONTROL PANELS

- a. Place power supply and associated hardware in same location.
- b. Label per LACCD labeling standards.

3. CARD READERS

- a. Wire the card reader using four conductor Telecommunications Industry Association / Electronic Industries Association (TIA/EIA) compliant RS-485 wiring to achieve secure encrypted communication using the latest Open Supervised Device Protocol standard.
- b. Readers shall be ordered with the optical tamper enabled.
- c. The card reader is to produce an audible beep tone to indicate to the user:
 - I. The card was read and/or access was denied.
 - II. Door is being held open and needs to be closed.
- d. Label per LACCD labeling standards
- e. Readers – must support HID iClass corporate 1000 series cards as well as any LACCD credential issued since 2008.
- f. Whenever possible, a single composite cable (“banana cable”) shall be utilized to connect door access control components to the door controller.
- g. All devices shall be homerun directly to the system / door controller.

4. DOOR HARDWARE

- a. Connect fire alarm output to the disconnect relay on the associated 24VDC lock power supply for fail-safe, egress-controlled doors only.
- b. Setup and conduct a door hardware coordination meeting.
- c. Coordinate the installation and termination of the security cable with the installation of the electric door hardware and transfer hinge.
- d. It is the intent of the District that all perimeter doors leading to areas containing classrooms or directly into classrooms shall be capable of remote lockdown from the existing District wide access control system.
- e. Provide cable and terminate wires to delayed egress devices for monitoring activation of delayed egress by the PACS system if applicable.
- f. Door magnet style locking hardware (Electro-Magnetic Locks or Maglocks) shall not be used without prior written approval from LACCD IS Department.
- g. All doors with card readers shall have a hydraulic closer installed.
- h. ADA Low Power Energy (LPE) doors where required shall include access control and proper peripherals equipment and the involved trades shall coordinate all aspects of the installation.
- i. All devices shall be homerun directly to the system / door controller.

LACCD Districtwide Security Performance Requirements

- j. Any new electronic access control installed on doors which fall under the prescripts of Chancellor's Directive 185 shall be capable of supporting both interior mechanical lockdown as well as remote electronic lockdown.

5. DOOR CONTACTS

- a. Install on protected (secured) side of door.
- b. Install 6" from leading edge at top of door.
- c. Perimeter door contacts shall be Double-Pole, Double-Throw (DPDT) to permit connections to both the Access control and Intrusion systems.
- d. Coordinate with the door frame supplier for location where the frame will be grouted.
- e. Whenever possible, a single composite cable ("banana cable") shall be utilized to connect door access control components to the door controller.
- f. All devices shall be homerun directly to the system / door controller.

6. REQUEST-TO-EXIT

- a. Mount motion detector on the secured (protected) side of door.
- b. Install motion detector so that detection pattern is not obstructed by Exit Signs, light fixtures and other objects that would interfere with proper operation.
- c. Set motion detector to a 1 second pulse.
- d. Mask detector lens to provide a confined detection area limited to the door handle or push bar.
- e. Whenever possible, a single composite cable ("banana cable") shall be utilized to connect door access control components to the door controller.
- f. All devices shall be homerun directly to the system / door controller.

7. LOCAL SOUNDERS

- a. Mount local alarm sounder as indicated on project drawings.
- b. Install local, square, and plumb. Set flush-mounted units so that the face of the cover, bezel, or escutcheon matches the surrounding finished surface.
- c. Mount so that there are no gaps, cracks, or obvious lines between the trim and the adjacent finished surface.
- d. All devices shall be homerun directly to the system / door controller.

8. SPARE PARTS

- a. The following spare parts shall be maintained on hand, by the integrator, for the length of the warranty period, with quantities specific to each project (fractions shall be rounded up to the nearest whole number):
 - I. 5% of the total number of card readers installed
 - II. 5% of the total number of reader interfaces of each type used
 - III. (1) ISC of each type used
 - IV. (10) of each type door position switch used
 - V. 5% of the total number of Request-to-exit sensors used

LACCD Districtwide Security Performance Requirements

- VI. (1) spare power supply of each type used
- VII. (1) spare Power distribution module
- VIII. (5) spare fuses of each type used

9. PACS INTEGRATION

- a. All intrusion functionality shall be monitored and controlled from within Alarm Monitoring in OnGuard.
- b. The Contractor shall perform all necessary programming in the PACS to accomplish this integration.
- c. If an area is armed, a code or authorized workgroup credential shall be required to disarm.
- d. When an area is armed, and someone enters the area the keypad shall audibly and visually indicate the entry warning signals.
- e. The system may be disarmed by presenting a valid PIN on the system keypad.
- f. The system may be armed or disarmed by presenting a valid authorized credential at a designated ARM/DISARM card reader located adjacent to the keypad.

End of Section