LOS ANGELES COMMUNITY COLLEGE DISTRICT

Districtwide Minimum Standards

for

Physical Access Control Systems

December 6th, 2018

LACCD Facilities Minimum Design Standards for Physical Access Control Systems (PACS)

Outline

The following document contains the deployment, technology, and installation standards for Physical Access Control Systems (PACS) within LACCD facilities.

Program managers, designers, and contractors shall review and familiarize themselves with the requirements contained herein prior to beginning any project which has a PACS component.

Table of Contents

Appendix

LACCD Facilities Minimum Design Standards for Physical Access Control Systems (PACS)

1. Summary

LACCD has developed standards governing the deployment of Physical Access Control Systems to provide a baseline level of security that is required within District facilities. The PACS standards were developed to meet the goals and recommendations as described within the following documents:

- Chancellor's Directive 185, Dated April 27, 2018 (Attached as Appendix 3)
- Blue Ribbon Panel on Campus Safety & Emergency Preparedness, Dated December 16, 2015 (Attached as Appendix 4)
- LACCD Strategic Plan 2018 – 2023, Dated January 18, 2018 (Attached as Appendix 5)

These standards shall be utilized to aid in the application of current technology standards and best practices to all new construction as well as renovation projects undertaken within the District.

A physical access control system is any system which manages access to areas through the issuance and revocation of entry credentials. The purpose of the PACS is to efficiently and effectively control access to buildings and rooms within buildings based upon 3 key principles:

- Who is allowed to enter controlled access areas
- Which areas they are allowed to access
- When they are allowed to access them

As an enterprise-level PACS is a complex system, with operating and supporting components which fall under the purview of disparate departments at both the District as well as the College level, the operation, oversight, and maintenance of the systems discussed herein is primarily the shared responsibility of the following (4) departments:

- Facilities
- Information Technology
- Administration
- Safety & Emergency Response

2. Acronyms Used

- IT – Information Technology
- IDS – Intrusion Detection System
- LACCD – Los Angeles Community College District
- PACS – Physical Access Control System (Building Access Control)
- PIN – Personal Identification Number
- REX – Request to Exit

3. Typical PACS Devices

The PACS consists of the following operating components:

- PACS Host Server – This is where the core system software typically resides, including the user database from which user workgroups and credentials are derived, as well as the actual operating software of the system.

- PACS Workstations – These are where system operators / administrators can alter system configurations, enter and delete users, modify access levels, monitor alarms and door positions, remotely release doors when appropriate, and perform all other operator / administrator related tasks.

- PACS Controlling Software – This is the actual operating system of the PACS. For the District standard of Lenel, it is the On-Guard platform.

- Door Controllers – This is where local decisions are made regarding the validity of a credential and if the credential should grant access to that particular door at that particular time. Door controllers should be able to function in an offline environment, where there is no connectivity to the host server, and log a minimum of 10,000 transactions. Transaction data shall upload, and any recent system changes should download as soon as host connectivity is restored.

- Card Readers – These are contactless devices which wirelessly read a user's credential, decrypt the credential identifier and transmit that credential identifier to the Door Controller for validation of access. Dual factor Authentication Card Readers shall also have an integral keypad to allow for Personal Identification Number (PIN) entry. Any card reader or card reader / keypad installed shall be capable of reading any non-proprietary LACCD proximity card or keyfob credential issued since 1998.

- System Credential - A Credential that is issued by LACCD for the purpose of allowing properly authorized individuals to access buildings and selected rooms within buildings. The type of credential can vary, and may include form factors such as proximity cards, multi-class smart cards, or keyfobs.

- Electronic Locking Hardware – This is the door hardware which physically secures the door and releases it for access upon presentation of a valid credential to the card reader.

- Request to Exit (REX) Sensor – This device allows users to exit through an access-controlled door without triggering a "forced door" alert which results if an access-controlled door is opened without presentation of a valid credential. It is typically either an integral part of the electronic door locking hardware or a separate device mounted above the secure side of the door.

- Door Position Sensor – This device monitors the door for opening and reclosing and will cause the system to alert if a door is opened without presentation of a valid credential or if the door is left open for more than 10 seconds after presentation of a valid credential.

4. District Standards for PACS Deployment

The LACCD has determined minimum levels of physical access control to be deployed at each LACCD College. The following door types are to be equipped with electronic access control and integrated into the District-wide PACS without exception:

- Any exterior door leading into a building containing classrooms.
- Any exterior door leading directly into a classroom. (This type of door shall also to be equipped with internal lockdown capability, with such lockdown to be independent of and not interfering with the operations of the District-wide PACS.)
- Any interior or exterior door leading into a room that contains valuable academic equipment or resources such as computer laboratories, instruments, tools, media equipment / materials, etc. All Childhood Development Centers shall be included.
- Any interior or exterior door leading into an area containing Critical Infrastructure, where unauthorized entry could drastically impact the daily operation of the college or cause great harm to an individual such as data closets, electrical closets, mechanical equipment rooms, fire suppression equipment rooms, roofs, and other inherently hazardous areas. These doors shall be secured via dual factor authentication such as card and PIN (keypad).
- Any interior or exterior door leading into any chemical laboratories, chemical storage rooms and any other rooms which contain dangerous substances that could harm an individual unfamiliar with the hazards such substances represent. These doors shall be secured via dual factor authentication such as card and PIN (keypad).
- Any interior or exterior door leading into an area containing file storage rooms that contain sensitive financial or personal information of individuals. These doors shall be secured via dual factor authentication such as card and PIN (keypad).
- Any interior or exterior door leading into a storage rooms that contain safes, large sums of cash, works of art, and/or other high value items. These doors shall be secured via dual factor authentication such as card and PIN (keypad).
- Any interior or exterior doors leading from a public space into the secured area of the Campus Safety location.
- Any interior or exterior door leading into evidence storage, weapons storage, quartermaster or other law enforcement equipment rooms. These doors shall be secured via dual factor authentication such as card and PIN (keypad).

5. Security System Integrations

- All PACS and IDS components shall be controlled by and report to a common enterprise level software operating platform, in order to facilitate the monitoring of

both technologies on a single workstation located within Campus Safety, as well as any other authorized location.

This software platform shall be compatible with, and capable of integration to, the current District-wide Lenel platform without exception.

- The Video Monitoring System (VMS) software platform shall be integrated into the PACS software platform in such a fashion as to cause selected PACS user actions and policy violations as well as IDS / Duress activations to be tagged with descriptive metadata on the recorded video and activate a live viewing screen.

  The integration shall also provide through the PACS a graphical layout of the floor plan with the location of all sensors shown, and any sensor in the alarmed state shown as blinking red to allow for ease of location.

6. Enterprise Software Capabilities

- The PACS system shall be configured as a centralized enterprise system using a District master server and local College servers.

- System operators and administrators of the PACS shall only be granted access to the application using Windows Active Directory credentials.

- Audit trail records shall be accurately maintained for a period of three (3) years of which individuals performed programming / configuration / database changes within the PACS as well as records of valid and invalid usage attempts from each card reader.

- The PACS shall integrate into the District HR system as to allow for credential issuance and revocation for new and terminated employees.

7. System Performance Verification Testing and Commissioning

- A performance verification testing and commissioning report shall be completed for each PACS project, containing a checklist of all District deployment and installation standards. This testing and commissioning process shall serve to verify compliance with all features and functionality required of the PACS. If any portion of the system fails the testing / commissioning process, the issue shall be corrected, and the process shall begin again. Any system consecutively failing (2) such testing attempts shall be retested at the Contractor's expense.

- A representative from each firm involved with any portion of the installation shall be present for the system testing in order to ensure whichever firm is responsible for the failure is present and able to resolve the issue expeditiously.

8. System Equipment, Installation and Configuration Specifications

- Refer to Appendix 1, Districtwide Security Performance Requirements, for additional details on the equipment and configuration settings that shall be utilized.

- Refer to Appendix 2 for typical installation details.

9. Training and Documentation

- Support and training costs associated with the PACS will be paid by the Software Installer.

- A minimum 16 hours of system training shall be allocated for each project containing greater than 25 access-controlled entrances. This training shall be conducted by a manufacturer authorized and certified instructor. Training materials shall be supplied in both printed as well as electronic format and shall be specific to the project.

- Training shall not begin until the PACS has been completely tested and commissioned, in order that users may be trained on a fully functional system.
- Training shall be centric to the operational roles that the College deems necessary at the time the training takes place.

- Training shall be formatted into 4-hour increments, so that multiple training sessions may take place depending upon the availability of the staff requiring the training.

10. Standardized Software Platform

- The LACCD PACS standard is the OnGuard Enterprise Access Control System as manufactured by Lenel.

END OF SECTION