LOS ANGELES COMMUNITY COLLEGE DISTRICT

Districtwide Minimum Standards

for

Intrusion Detection System

May 30, 2019

Outline

The following document contains the deployment, technology, and installation standards for Intrusion Detection Systems (IDS) 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 an IDS component.

Table of Contents

Strategic Documents

1. Blue Ribbon Panel on Campus Safety and Emergency Preparedness
2. LACCD 5-Year Strategic Plan 2018 – 2023

1. Summary

LACCD has developed minimum design standards governing the deployment of Intrusion Detection System (IDS) components to provide a baseline level of security that is required within District facilities. The IDS standards were developed to meet the goals and recommendations as described within the following documents:

A. Blue Ribbon Panel on Campus Safety & Emergency Preparedness, Dated December 16, 2015 (Attached as Appendix 1)
B. LACCD Strategic Plan 2018 – 2023, Dated January 18, 2018 (Attached as Appendix 2)

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

An Intrusion Detection System monitors a designated area/zone for activity during certain periods of time and is either automatically monitored during a preconfigured schedule or activated/deactivated by an authorized individual using a unique pin code and/or credential.

Intrusion detection is best achieved with multiple types of sensors that can capture and report activity in real-time to alert a monitoring station of activity. Using card readers and surveillance cameras allows authentication and visual verification to take place and allows for greater situational awareness then what many other IDS components typically provide. Thus, it is recommended to utilize these components when possible and use other IDS components only in select areas where additional monitoring is required.

The operation, oversight, and maintenance of the systems discussed herein is primarily the shared responsibility of the following departments:

A. College Administration (IT and Facilities)
B. Campus Safety Office
C. District Information Technology
D. District Safety and Emergency Services

2. Acronyms Used

A. IDS – Intrusion Detection System
B. IT – Information Technology
C. PACS – Physical Access Control System
D. RF – Radio Frequency

3. Intrusion Detection System Components

A. Dual Technology Motion Detectors – Devices which detect the presence of body heat and motion via thermal and RF volumetric sensor technology.
B. Glass Break Detectors – Devices which detect the specific frequencies of breaking glass.

C. Magnetic Contacts – Devices which detect the opening and closing of a movable object such as doors, windows, and access hatches.
D. Arm / Disarm Keypads – Devices used for arming and disarming individual alarmed areas/zones.
E. Duress (Panic) Buttons – Devices which allow an individual to press a button to send an alert to a monitoring station.
F. Input / Output Control Boards – Device used for interfacing sensors with the Physical Access Control System.
G. Notification Appliances – Device used to provide local audible and / or visual indication of an alarm condition.
H. Monitoring Station – Workstation and software capable of receiving and displaying alarm inputs in a manner that facilitates immediate response from the individual responsible for the monitoring. This will allow for local alerting as well as data push to any mobile / smart devices authorized to access system data.

4. Intrusion Detection System Technical Standards

The District-Wide IDS and all associated components shall meet the following minimum requirements:

A. Shall interface natively with the Video Management System with no need for custom integration or third-party equipment or interfaces.
B. Shall utilize the Physical Access Control System and the Video Surveillance System as a medium for displaying alerts to a monitoring station.
C. Shall be capable of utilizing video surveillance cameras instead of and in addition to other IDS sensors for motion detection.
D. Shall utilize device supervision to ensure no communication disruption occurs between the monitoring station and each IDS sensor.
E. Sensors shall be capable of being monitored individual or assigned to zone(s) and monitored as a group depending on the needs of the stakeholders.
F. Shall be cabled to the nearest PACS enclosure utilizing cable which meets the manufacturer's recommendation as well as any applicable LACCD standards.
G. Shall have a minimum of six hours of backup power available in the event of primary power interruption.
H. Pin codes and / or credentials utilized for arming/disarming zones shall be unique to each individual. The transmission of these credentials shall be encrypted.

5. Standards for Intrusion Detection System Deployment

Each project involving IDS components shall include a detailed requirement gathering process to determine what equipment is required and how it shall be operated. While the preference is to utilize card readers and surveillance cameras to meet the security needs whenever possible, areas that may require additional IDS components are listed below.

A. Arm/Disarm Keypads shall be provided in the following places:
    a. Areas/Zones that require IDS sensors, but regular monitoring hours cannot be determined for automatic arming and disarming.
    b. Areas/Zones that require individual control of arming/disarming outside of regularly scheduled monitoring.
B. Magnetic Contacts shall be provided in the following places:
    a. All exterior building doors.
    b. Any doors with controlled access through the PACS.

c. Access hatches or doors leading to a building's roof or other dangerous area not adequately protected by the PACS or a video surveillance camera.
d. Operable windows on the ground floor where an individual may be able to traverse into a building without using a door.

C. Glass Break Sensors shall be provided in the following places:
a. Areas/Zones containing extremely valuable assets that could be accessed from the exterior of the building by breaking a pane of glass.

D. Dual-Technology Motion Detectors shall be provided in the following places:
a. Areas/Zones where a Video Surveillance Camera cannot be mounted due to privacy concerns, but motion detection is still required.
b. Areas/Zones containing extremely valuable assets that would benefit from both cameras and dedicated motion detection sensors.

E. Duress (Panic) Buttons shall be provided in the following places:
a. Areas/Zones where large sums of cash are handled.
b. Areas/Zones where disciplinary functions are handled
c. Executive staff offices.

6. System Integration Capability

A. IDS system components shall utilize the VMS for all functions including monitoring, arming/disarming zones and recording alarm activations for future reporting, but shall also be capable of integration with the Physical Access Control System to enhance functional capabilities as required.
B. IDS components shall be operable and monitorable through the LACCD standard Video Management System through a graphical user interface map of each building so that individuals monitoring the alarm can easily identify the exact location of the activated sensor.
C. Activation of an IDS sensor shall automatically be recorded in the VMS as well as bookmark associated video feeds so that activations can be quickly investigated.

7. System Performance Verification Testing and Commissioning

A. A performance verification testing and commissioning report shall be completed for each IDS 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 IDS. 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 two (2) such testing attempts shall be retested at the Contractor's expense.
B. 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. Training and Documentation

A. Training in the operation of intrusion detection equipment shall be a component of the access control system training.

9. Warranty

A. All intrusion detection equipment shall be warrantied against any defects in material and workmanship under normal use for a period of five (5) years from date of official acceptance of the completed project by the Owner. The Vendor shall complete a manufacturer "Installation Certification" certifying the date on which the system has been installed to ensure the Owner receives full warranty rights from the manufacturer.

END OF SECTION