ADMINISTRATIVE MEMORANDUM

COUNTY OF SAN MATEO

NUMBER: B-30

SUBJECT: Electronic Security System Standards

RESPONSIBLE DEPARTMENT: County Manager / Clerk of the Board

APPROVED: _____ **DATE**: 11/14/19
Michael P. Callagy, County Manager

I. Overview

The County of San Mateo strives to secure its facilities while maintaining appropriate public access. To do this, the County's various departments may elect to install electronic security systems, including systems that include security controls employing electronic monitoring, intrusion systems, and/or panic or status alarm services. To ensure interoperability and consistency across County sites, it is essential that any electronic security system meet the County operational, technological, and legal standards set forth in this Policy.

II. Policy Purpose

The purpose of this standard is to implement a uniform set of practices and protocols governing the implementation of physical security components that include the design, specification, installation, testing, acceptance, maintenance, and operation of electronic security systems within or around the County's campuses and facilities. This policy is not intended to mandate security systems in County-owned or -leased facilities. The goal is to ensure that installations of new systems or upgrades to existing systems deemed appropriate by the Building Security Working Group (BSWG), the Sheriff's Countywide Security Unit and/or County department(s), meet the minimum standards contained herein and are compatible with existing component systems (i.e., alarm, monitoring, etc.).

III. Scope

This standard applies to all County-owned facilities as well as leased buildings. However, alternative security measures, including contract security monitoring services, may be considered for outlying facilities, as well as those facilities deemed temporary or scheduled for

replacement in the near-term, where new installations would not be in the best interest of the County. This policy is prospective in nature and does not require the replacement of existing systems that are in good working order and continue to achieve their intended purpose.

IV. Policy

This standard serves as the basis for all electronic security implementations. The criteria described in this document are the standards that shall be applied to all San Mateo County building projects. The design and implementation of an electronic security systems can vary dramatically. Each implementation may be customized or tailored to meet specific security objectives of the department. To assist in defining these objectives, the initiating department should consult with the Sheriff's Countywide Security Unit, Department of Public Works (DPW), and Information Services Department (ISD) for recommendations. Furthermore, the Sheriff's Office County-wide Security Unit shall be notified and invited to an initial design meeting during the schematic design process of any new or remodeled County building project to assess the need for security electronics implementation. Unique applications may also require engaging a security consultant.

A. Process for New Additions, Modifications, or Removal

Departments shall initiate any modifications to the County's existing security system (JCI/P2000) through the County's Service Desk Ticketing System (ServiceNow). This includes additions to and elimination of existing systems and/or hardware.

B. Electronic Security Systems

Security electronics systems shall be non-proprietary and shall be integrated and communicate via the County's network. Security electronics systems may include any of the following components:

1. Card Access Control

The Card Access Control System shall be the primary means of monitoring security events, controlling card access points, as well as logging and reporting activity.

- New card access control equipment must be configured/connected to an existing County access control system, communicating via the County-wide network and not implemented as a stand-alone system unless approved in advance by the Sheriff's Countywide Security Unit.
- Administration of the Card Access Control System shall occur at designated and secured client computers.
- Card access control system design shall restrict access from a lower security area to a higher security area and provide access where the measures will substantially benefit operations and minimize issuance of keys.
    - Per code requirements, card reader doors shall always remain unlocked in the egress direction. Depending on security risks as determined by the Sheriff's Countywide Security Unit, some doors

may include egress alarms. This may not apply to institutional facilities, such as adult corrections, the juvenile hall and other facilities that house County clients.

- Provide a multiclass card reader with a broad array of 13.56 MHz high frequency and 125 kHz low frequency credential technologies. Check with DPW on the specific models that can be installed in County facilities.
- Provide a request-to-exit (REX) switch in the door hardware, wall-mounted REX push button or above-door REX motion sensor to bypass the door position sensors and allow movement from the secure side of the door to the unsecure side of the door without generating an alarm at all card-access-controlled doors.
- Doors, hatches, and other exterior operable access points not connected to the card access control system via a card reader shall be monitored with an electrified position switch device for forced entry.
- Provide a Digital Alarm Communicating Transmitter and associated outside phone line connections for communication to a third party central station in each building.
- Perimeter door alarms shall have a local Digital Alarm Communicating Transmitter for after-hours monitoring capabilities.
- Connect card Access Control System controllers and lock power supplies to emergency power (ePower) circuits unless e-power is unavailable.
- Provide card Access Control System interface with video surveillance system to provide automatic camera video association with the Card Access Control System alarm events including door forced, invalid card read, and duress alarm activation.
- Provide battery backup with 1-hour minimum runtime for each Card Access Control System controller, plus an additional 25 electrified lock activations for each lock connected to a lock power supply. Card Access Control System controllers connected to ePower circuit will only require 15 minutes of battery runtime plus an additional 25 electrified lock activations for each lock connected to a lock power supply.
- Contractor will be responsible for providing initial programming for new access control installations, connecting the equipment and ensuring successful network communications. The department charged with oversight and/or administration of the cardkey system will be responsible for setting security access levels for each new device.

2. **Video Surveillance**

- Provide self/software focusing IP-based color cameras capable of recording a minimum of 1080 pixel resolution, 30 frames per second. Provide RAID-6 data storage capacity to meet the minimum County retention requirements, plus an additional 15%.
- Cameras shall be programmed to record at a minimum 720-pixel resolution, 10 to15 frames per second, for 365 days with storage conforming to countywide security standards and data retention policies. Day/Night

cameras will be used at exterior locations with a minimum color illumination of 0.1 Lux.

- At a minimum, recording may be set to record on motion only. Video capture shall be tested on a regular basis to ensure that the system is capturing the intended footage.
- Camera shall be powered via a Power over Ethernet (PoE) network switch or by a Class 2 camera power supply providing the power supply has a separate circuit breaker or fuse-protected output for each camera powered. The PoE switches will either be provided by ISD or meet ISD approved standards.
- Cameras or security devices connected to the network must be approved by the Information Services Department.
- Video Surveillance System equipment provided for new projects will be compatible with and viewable on existing video surveillance system video client workstations in the designated Sheriff's Operations Center location(s). Departments may request an exemption that cameras not be actively monitored as long as the retention requirements contained herein are met. Such requests must be made to the Building Security Work Group prior to installation.
- Provide an uninterruptible power supply (UPS) with 1-hour minimum runtime for each camera PoE switch and each camera power supply.
- A single UPS shall be used for all camera system components in the same room.
- Camera system components shall be connected to ePower circuits where available.
- Camera system components connected to emergency power circuits shall require 15 minutes of UPS runtime.

3. **Duress Alarm**

- Duress alarm push-buttons shall be connected to Card Access Control System alarm inputs for event reporting.
- Duress alarms located on counters with public/staff interactions shall have camera coverage on the public side.
- Duress alarm Push-button alarms shall be transmitted to a third-party central station via a local digital alarm communicating transmitter in each building.

4. **Intrusion Detection**

- Where an intrusion alarm system is included in the security electronics design, monitoring of perimeter doors shall be provided.
- Provide a double-pole door position switch at each door monitored simultaneously by the access control and intrusion detection system.
- Provide a keypad arming/disarming stations at the building interior near the staff entry locations.
- Provide a Digital Alarm Communicating Transmitter for connection of Intrusion Alarm System to a third-party central station for alarm monitoring.

This does not include institutional facilities, such as adult corrections, the juvenile hall and other facilities that house County clients.

5. **Cable Routing**

- Follow the County's telecommunication infrastructure design guidelines for all cable routing.
    - Route all security cabling in metallic conduit or raceway where run in walls and above hard ceilings. Above accessible ceilings, utilize cable tray where provided and J-hooks elsewhere.
    - Ensure cable is listed for its intended application.
    - Provide back boxes suitable for all field devices and terminations.
    - Flush-mount Security electronics devices where possible.

C. **Security Device Location Requirements**

1. **Building Exterior**

- Provide a Pan-Tilt-Zoom camera, building attached, for active monitoring of public events where a plaza or public gathering location is established between, or adjacent to County buildings.
- Provide a pedestal-mounted card reader for vehicle entry where a vehicle gate or barrier arm is used to secure a driveway or parking entrance for County personnel access.

2. **Building Envelope**

- Provide a fixed-view exterior camera at building entrances and exits.
- Provide an electronic door position monitoring and local door alarm sounder at each building emergency exit door.
- A card reader shall be installed at each building staff entry door.
- Provide a building intrusion alarm connected to a third party central station for after-hours building monitoring at buildings that are not generally staffed after normal business hours where staff can easily verify the last person out of the department at the end of a business day.

3. **Lobby, Circulation, and Waiting Areas at HOJ**

- Provide fixed-view camera coverage in the lobby, circulation, and waiting areas
- Provide fixed-view camera coverage of the screening area with camera view of each lane from the secure side of the magnetometer. Provide camera views of package weapons scanner screening lanes, and the exit side of the magnetometer checkpoint area.
- Provide a duress alarm pushbutton for each security lane.
- Provide fixed-view cameras with coverage of the exit lane from the non-secure side of the exit, and at exit lanes with secure turnstiles in-line with the screening lanes.

- Provide a card reader with electrified door strike or electric lockset at each door separating public space from staff space with a fixed-view camera coverage of the door portal from the unsecure side of the door.
- Provide a remote door release in direct view of the door at the staffed receptionist behind a secure transaction window in the waiting area.

4. **Parking Area Alarm Box or Call Station**

- Parking area emergency call boxes shall consist of an emergency, pushbutton-activated, automatic-dial telephone, and a blue light that activates on alarm condition.
- Provide emergency call boxes at each stairwell and elevator landing.
- Provide emergency call boxes, for exterior parking lots, to ensure at least one call box is visible to a pedestrian standing in the general parking lot area; excluding parking stall spaces.

5. **Public Transaction Counters**

- Provide a duress alarm pushbutton at each public transaction counter position.
- Provide an overall fixed-view camera with coverage of the public queuing and walk-up areas.
- Cameras behind transaction counters are not permitted if said cameras can pick up confidential information contained in documents.

6. **Staff/Client Meeting Rooms**

- Provide a duress alarm pushbutton in each mediator office.
- A fixed-view camera shall be installed with coverage in the corridors directly adjacent to mediator offices.

7. **Child Waiting**

- Provide a duress alarm pushbutton at the staff location inside of the child waiting area.
- Provide a fixed-view camera with coverage of the child waiting area; including interior and exterior corridors by the child waiting area door.

8. **Public Records Viewing Areas**

- Provide a duress alarm pushbutton at each staffed position in public records viewing areas.
- Provide a remote door release from a secured staffed position in direct view of the door where public records rooms are not staffed.
- Provide a fixed-view camera with coverage of all public records viewing areas.

9. **Loading Dock, Receiving, and Mailroom**

- Provide a card reader with electrified door strike or electric lockset at the loading dock and mailroom door entrances.
- Provide a fixed-view camera with coverage of loading dock and receiving areas.
- Provide a fixed-view camera and duress alarm pushbutton with coverage in the mailroom.
- Provide a hands-free ring down telephone outside the receiving door to facilitate communication with delivery drivers when loading dock and mailroom are closed.

10. **Security Equipment Location**

- Locate all electronic security control equipment, including computers, storage, interface equipment, etc., in a secure location with computers and storage equipment located in one of ISDs data centers.
    - Locate other security equipment, such as interface equipment, panels, and UPSs in building telecommunications rooms.
- Provide an enclosed and lockable equipment racks and/or wall cabinets for security control equipment.
- Coordinate all networking requirements of electronic security system control equipment with ISD.
    - All security electronics control equipment shall communicate over the San Mateo County WAN and conform to ISDs network design and security guidelines.

D. **Exemption**

Existing security components are grandfathered in if they do not currently meet this standard; however, when a change to a system is being made or when there is an unequal application of security controls, the deficiency must be corrected.

New requests for an exemption from these standards must be obtained from the County's Building Security Workgroup prior to project approval.