PURPOSE

The purpose of the San Diego County Security Policy has four elements:

1. To provide a safe and secure environment for all persons, both County employees and the public, at County owned or operated facilities;
2. To prepare County employees to report security concerns, violence, and threats of violence in the workplace;
3. To protect County owned and County operated property from damage, loss or destruction;
4. To protect the personal property of County employees and the public while conducting business at County facilities.

BACKGROUND

The County of San Diego has a long history of providing a safe and secure environment for County employees and the public that we serve. The County has a long-established policy prohibiting threats, violence and weapons in the workplace. (See Board policy A-121 Violence and Threats in the Workplace: Zero Tolerance and the Department of Human Resources Policy-1104 Workplace Risk Assessments). Penal Code section 171b outlines the prohibition of weapons within any state or local public building, including County owned and operated property.

In December 2015, the San Diego County Chief Administrative Officer authorized a comprehensive review of security protocols at all San Diego County owned and occupied facilities. The purpose of this review was to enhance security at County facilities with the ultimate goal of protecting County workers, County property and the public who utilize County facilities. The security initiative that emerged involves prevention, deterrence and mitigation.

SCOPE

The County security policy covers all County owned and occupied property. All County employees, while on duty and conducting County business, are subject to the requirements of the County security policy whether on County property or elsewhere.

POLICY

It is the policy of the Chief Administrative Officer to establish and implement a uniform and ongoing process to address the planning for and reporting of active threat events within County owned or controlled buildings. These procedures are designed to protect employees, residents and their property.

PROCEDURES

Each Deputy CAO shall designate a **Group Security Coordinator** who will be responsible for coordinating security programs and initiatives in their respective group.

Each Department Head shall appoint or assume the role of **Department Security Manager**. This person will designate a **Site Security Coordinator** at each County facility or location within their department and the Coordinator shall convene a **Site Security Management Team.** The Management Team will meet at least twice each year to address security issues for sites housing more than 50 employees and at least once per year for sites with less than 50 employees.

Vulnerability Assessments shall be conducted at all County facilities. These surveys shall be conducted by law enforcement trained personnel under the guidance and direction of the Law Enforcement Coordination Center / Critical Infrastructure Protection Program, in coordination with the Group Security Coordinator. Vulnerability Assessments shall be conducted:

a. When a new facility is opened or occupied;
b. When significant modifications are made to an existing facility;
c. Every five years.

Upon completion by law enforcement, the Assessments will be provided to the Group Security Coordinators who will facilitate dissemination to the Site Security Coordinators.

The Vulnerability Assessment is a confidential document per County Administrative Manual Item 0400-11 and is exempt from public disclosure per Government Code section 6254(f) and 6255. The Vulnerability Assessment shall always be locked in a secure place when not being reviewed. The Vulnerability Assessment shall not be shared unless there is a valid and articulable need to share the assessment.

Vulnerability Assessment Review & Security Action Plan

Within 30 days of receiving the Vulnerability Assessment, the Site Security Coordinator shall convene the Site Security Management Team to review the Assessment. All departments located on the property should have a representative on the Site Security Management Team.

The Site Security Management Team may include the following:

1. The Site Security Coordinator;
2. The San Diego-Law Enforcement Coordination Center Deputy, or Deputies, who completed the Vulnerability Assessment;

3. The Department of General Services facility and security lead;
4. Information Technology, if applicable to the results of the assessment;
5. Financial Services, if applicable to the results of the assessment;

The Site Security Management Team shall develop a written Security Action Plan, utilizing the County-approved, standardized format. The Security Action Plan shall address each of the suggestions from the Vulnerability Assessment. The plan shall include a proposed course of action, funding, timeline and the person responsible for completing the recommended action. As deemed necessary and appropriate, Department Heads may send drafts of Security Action Plans to County Counsel and Human Resources Risk Management and Training for review.

The Site Security Coordinator shall ensure the Security Action Plan is completed *within 90 days of receipt* of the Vulnerability Assessment, including review and approval by the Department Security Manager, Department Head, Group Security Coordinator and DCAO, as appropriate. After approval, the Security Action Plan will be sent to the OES Coordinator.

The OES Coordinator shall store an electronic copy of the plan in a CONFIDENTIAL, limited access, electronic file. The OES Coordinator will keep track of the status of all Vulnerability Assessments, Progress Reports and Security Action Plans.

The Site Security Coordinator shall submit progress reports every 180 days to the Department Security Manager. The Progress Report shall document completed actions, incomplete actions and obstacles to completion. The Department Security Manager shall review and forward the progress reports to the Group Security Coordinator. Group Security Coordinator shall review and forward the Progress Report to the OES Coordinator. Once a year, the DCAOs will update the CAO on the status of their Security Action Plans.

The Security Action Plan is a confidential document per County Administrative Manual Item 0400-11 and is exempt from public disclosure per Government Code section 6254(f) and 6255. The Security Action Plan shall always be locked in a secure place when not being reviewed. The Security Plan shall not be shared unless there is a valid and articulable need to share the plan.

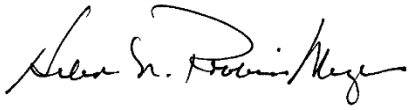
When a new facility is planned, the facility planning and development committee should invite participation from a representative of the Sheriff's Crime Prevention Unit and the Law Enforcement Coordination Center / Critical Infrastructure Protection Program.

New facilities, where practical, should incorporate Crime Prevention through Environmental Design principles and the security measures recommend by the LECC Critical Infrastructure Protection program.

Employees play an important role in maintaining safety and security in the work environment. Employee(s) should call 9-1-1 when there is immediate danger to County employees, the public or County property.

Department Heads should make employees aware of policies or protocols for communicating general security concerns, in addition to departmental protocols for contacting Risk Management (Department of Human Resources) to report threats to or by County employees, assaults on County employees, or significant damage/loss to County property. Threats or assaults to sworn law enforcement personnel to include deputy sheriffs, probation officers, and district attorney investigators shall be handled in accordance with their respective department procedures.

Approved:



Helen N. Robbins-Meyer
Chief Administrative Officer

Responsible Department(s)
Office of Emergency Services

ATTACHMENTS
N/A

CROSS-REFERENCES
Board of Supervisors Policy A-121

Department of Human Resources Policy 11-4