Facility Security

306.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the safety and physical security of all [City_County] facilities. Additional guidelines can be found in the Key and Electronic Access Device Controls Policy.

For information related to the protection of information systems and information technology infrastructure, see the Information Technology Use and Cybersecurity policies.

306.2 POLICY

It is the policy of the [City_County] to provide physical security measures to safeguard facilities under [City_County] control.

306.3 SECURE FACILITY ACCESS

All [City_County] facilities that are not open to the public should be equipped with self-closing and self-locking exterior doors. All exterior doors should remain closed and locked at all times, unless secondary barriers are in place or a [City_County] employee is present to prevent unauthorized access. Other points of entry to the [City_County] facility and all exterior units, including storage rooms and lockers, should remain closed and locked unless directly monitored by a [City_County] employee.

The [CM_CA] or the authorized designee should develop and implement a process for vendor and contractor access to secure facilities.

306.3.1 PUBLIC FACILITY ACCESS

All [City_County] facilities with public access should remain open and accessible during established business hours. All exterior doors that do not provide public access should remain closed and locked at all times. Each facility should maintain a designated reception area or secondary barriers to prevent unauthorized access to restricted areas. Restricted areas should be clearly and prominently marked. Sufficient staffing should be available to monitor visitor movement and prevent access to restricted areas (see the Public Safety Video Surveillance System Policy).

The [CM_CA] or the authorized designee should develop and implement a visitor control process for each [City_County] facility that allows public access.

306.4 SUSPICIOUS ACTIVITY

[City_County] employees should remain vigilant for any suspicious activity occurring in or around [City_County] facilities and should promptly report any such activity to a supervisor. Suspicious activity may include but is not limited to:

- Anyone loitering in the vicinity of the facility for an extended period of time.
- Unauthorized individuals photographing or taking images of the facility, employees of the [City_County] assigned to the facility, or [City_County] vehicles.

- Unknown individuals who appear to be monitoring the activities taking place at the facility.
- Anyone attempting to gain access or requesting access to [City_County] facilities without proper authorization.
- Any unknown or abandoned packages, vehicles, or other items left on [City_County] grounds or adjacent to [City_County] facilities.
- Unmanned aerial systems (drones) operating over or near [City_County] facilities without authorization, especially when hovering, filming, or flying at low altitudes.

306.5 THREATS AGAINST [CITY_COUNTY] FACILITIES

If a [City_County] employee receives a threat against a [City_County] facility that presents immediate danger (e.g., bomb threat, active shooter, other imminent risk to life or safety), the employee should obtain as much information about the threat as reasonably possible and immediately contact law enforcement. As soon as practicable afterward, the employee should notify the [DepartmentHead], who will notify the [CM_CA].

If the threat does not pose an immediate danger, the employee should obtain as much information about the threat as reasonably possible and promptly notify the [DepartmentHead], who will notify the [CM_CA]. The [DepartmentHead] or the [CM_CA] will notify law enforcement and assist with coordination, if requested.

306.6 BREACH OF SECURITY

Any breach in security at a [City_County] facility should be immediately reported to a supervisor, who should address the incident and report it to the [DepartmentHead].

If the breach presents an active or imminent threat to safety, the employee should first contact law enforcement, then notify the [DepartmentHead] as soon as practicable.

In either case, the [DepartmentHead] will notify the [CM_CA] of the breach.

306.6.1 POST-INCIDENT REVIEW

In the event of a breach in security at a [City_County] facility, the [CM_CA], the [DepartmentHead], or an authorized designee should conduct a post-incident review to evaluate the nature of the breach and determine appropriate follow-up actions based on the level of risk involved.

306.7 BUILDING EVACUATION PLAN

The [CM_CA] or the authorized designee should establish a general evacuation plan for each [City_County] facility for use during any emergency requiring the evacuation of employees or the public. The plan should include clearly marked exits, evacuation maps, and specific instructions for assisting individuals with disabilities.

In the event of an evacuation, all employees should follow the established evacuation plan and comply with posted exit strategies.

See the Emergency Management Plan Policy for additional guidance.

306.8 SECURITY ASSESSMENTS

The [CM_CA] should designate an employee or external consultant to periodically conduct facility risk assessments to identify vulnerabilities and improve security plans.