Security Procedure

Policy: See N-06 Physical Access Controls at www.cosdcompliance.org

Definitions: See HHSA Policy N-13 Security Definitions

Procedures:

A. Personnel Access Controls

1. County ID badges must be worn where visible at all times while conducting County business.
2. Report to your manager/supervisor any individuals in restricted work areas who are not escorted or authorized to be in the secured area.
3. County ID Badges coded for building(s) access must be granted at the minimum necessary or as required by the employee's job function(s).
    - Building access is to be removed in a timely manner when no longer needed such as when the employee transfers out or terminates County employment.
4. County ID badges are not to be shared with anyone

B. Building Access Controls:

1. Restricted work areas are to be secured to allow access to authorized individuals only. One or more of the following may be used to prevent unauthorized access to the work area where Protected Information is received, processed, stored, or destroyed:
    - Secure building with badge access
    - Cipher or combination lock
    - County ID badge to be visible at all times
    - Counter / reception desk for visitor sign-in (visitor badge)
    - Escort visitors in restricted areas
    - Security guard(s)
    - Security cameras
    - Alarm system for restricted areas

2. Cipher or combination locks that allow access to internal entrances to restricted work areas or external entrance to the County facility must be changed at least on an annual basis.
    - The code/combination is to be treated as a password and is not to be shared with anyone outside the office group or without the consent of your manager/supervisor.
3. Access to storage rooms is to be limited to authorized users with a business need only.

C. Workstations

1. Desktops are to be locked, logged off, or shut down when left unattended.
    - For desktops located in a public area, position screen monitors to preclude observation by unauthorized individuals.

2. Laptops are to be kept in a locked drawer or cabinet when not in use unless it is physically secured with a cable lock or is located where sufficient physical controls are in place to protect it from unauthorized access.

D. Social Engineering

Be aware that an unauthorized individual can pose as an authority figure using trickery or deception to enter a restricted area or gather personal or confidential information. If a stranger is requesting access to a secured area in the facility, and cannot provide you with a known contact person's name, work order, or valid ID badge, do not let the person in or provide them with any sensitive information. Immediately notify your manager/supervisor and/or the security guard for assistance.

E. Facility Security Incidents

For work order requests or in case of a facility security incident (e.g. vandalism, break-in, theft) contact HHSA Facilities Management Unit at (619) 692-8279 or FacilitiesMGT.HHSA@sdcounty.ca.gov to provide assistance as needed.

F. **Facility Evacuation or Re-entry in the Event of an Emergency**

HHSA Programs shall follow the procedures identified in their Continuity of Operation Plan (COOP) and/or the Site Evacuation Plan (SEP) for facility evacuation and re-entry in the event of an emergency.

Violations or suspected violations of this policy will be referred to the Agency Human Resources for appropriate personnel action or investigation.

QUESTIONS/INFORMATION: HHSA Information Security Manager at 619-338-2634