Title VI – Information Services

Section 474 – Media Protection Policy

Overview: This county-wide media protection policy shall be implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media as well as guidelines for reuse, disposal, or destruction.

Purpose: The purpose of this policy is to outline the proper use, disposal, sanitization, and/or destruction of media whether electronic or physical. There are special handling requirements for sensitive or classified data and media. Inappropriate handling may put the County, its constituents, its vendors, or County workers at risk.

Scope: The policy will both directly and indirectly impact all county workers, including non-employees and third parties who access county information systems. This policy applies to all data owned by or administered by the County of Santa Cruz as well as third party devices and/or registered personally owned devices used to access confidential county data (including but not limited to: HIPAA, payroll, personnel, client PII, or DOJ data).

Policy:

1. Media Storage and Access: Controls shall be in place to protect electronic and physical media while at rest, stored, or actively being accessed.
    a. “Electronic media” includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” includes printed documents and imagery that contain confidential county data.
    b. Controls include administrative, technical, and physical safeguards, such as restriction to authorized personnel and use in secured areas
    c. Media should be appropriately marked, labeled and documented for asset tracking and to avoid comingling of data.
    d. Record storage is in compliance with County Records Retention Policies, Title IV – Records Management Section 300 Retention.
2. Media Transport: Controls shall be in place to protect electronic and physical media while in transport (physically moved from one location to another) to track chain of custody and to prevent inadvertent or inappropriate disclosure and use.
    a. Data shall be protected using encryption when possible using the applicable standards.
    b. Pickup, receipt, transfer and delivery of such media shall be restricted to authorized personnel.
    c. A locked briefcase or lockbox should be used to secure confidential electronic or paper documents awaiting, or during transportation

    d. Workers must never leave any media unattended in a vehicle, public places or any non-county facility, this includes “checked luggage” when travelling.
3. Media Sanitization and Disposal: Controls shall be in place to safeguard data and electronic media prior to reuse, release out of organizational control, disposal or destruction. Santa Cruz County has the ability to perform these functions in-house for county-owned assets.
    a. Maintain written documentation of the specific steps to be taken to securely sanitize or destroy electronic media, compliant with the applicable regulations for the information type contained.
        i. Specific procedures shall be based on the information type contained on the media and the applicable regulations.
        ii. Documentation may include checklists, chain of custody, witnesses, and records of destruction.
        iii. Certificates shall be provided as verification of the procedure and efficacy.
        iv. Devices that are not technologically capable of being sanitized for reuse shall be overwritten or destroyed.
    b. County shall require destruction of media contained in equipment owned by others (such as hard drives in copiers or data stored on registered personal devices) as outlined in this policy with appropriate destruction documentation.
    c. Physical media shall be securely disposed of when no longer required, using the formal procedures noted in the Destruction of Records policy, Title IV – Records Management Section 400 Destruction. http://sccintranet.co.santa-cruz.ca.us/Departments/Personnel/Procedures-Manual
4. Notification and Reporting: Incidents resulting in the loss of or unauthorized access to data devices must be reported to the appropriate County IT support desk or as directed by departmental policy.
5. Roles and Responsibilities: Workers must use caution at all times to safeguard electronic and physical media against improper access or use.
6. Penalties: Violation of any of the requirements in this policy by any County worker will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution, and / or termination.