Title VI – Information Services
SECTION 469 – Data Access Policy
Latest Update: June 2024

A. OVERVIEW

This policy outlines the rules and responsibility for sharing electronic information between and among departments in the County of Santa Cruz. By promoting collaboration and information sharing, the policy aims to enhance decision-making, streamline operations, and improve service delivery while ensuring the protection of sensitive information and compliance with applicable legal, regulatory, and ethical standards.

B. PURPOSE

The purpose of this policy is to:

1. reinforce that existing standards and policies regarding professional conduct also apply to computer usage.
2. protect County data and computer systems from intentional misuse
3. ensure that County data and records are properly managed and secured for efficient, and lawful exchange of data between and among departments.

C. SCOPE

This policy applies to all County employees, interns, contractors, and all other users of County computers and computer systems.

D. DEFINITIONS

- **Custodial** - Refers to the role of a data custodian, which is the primary responsibility of managing the technical aspects of data storage, security, and access, ensuring its safekeeping and integrity by implementing controls like access restrictions, backups, and data quality checks, while adhering to data governance policies; essentially, they are responsible for the technical "care" of the data within an organization, without necessarily owning the data itself.

- **Custodian of records** - A "custodian of records" refers to the person or entity designated to be responsible for the safekeeping, management, and control of official documents, records, or information within an organization, including ensuring their proper storage, access, and destruction when necessary; essentially, the person who is in charge of maintaining and overseeing all records within a given entity

- **Data owner** - A data owner is a person or group, such as a department or division, that manages and is responsible for data within an organization. They are responsible for the accuracy, integrity, and use of the data.

E. POLICY STATEMENTS

1. Ownership

Each piece of data kept in the County's data repositories or provided over the County's data network is controlled and maintained by a specific department. As the data owner, this control department has the authority to control access to the data.

2. Custodial Responsibility

The Information Services Department has custodial responsibility for data in the County's data repositories, or provided over the County's data network while it is on the network. Custodial responsibility also exists within the Department of Community Development and Infrastructure, Human Services Department, and Health Services Agency over data in their data centers or cloud-based systems. This custodial responsibility does not include authority to release the data or provide access to it. Information Services is not the controlling department for any data, except data that supports internal Information Services operations and contains no information controlled by another department.

3. Security

The Custodial Department is responsible for administering security and data controls per County Procedures Manual Section VI - 440, County Ownership and Access to Computer Data, Files, and Software.

4. Requests

This policy provides the procedure for the "request and consent" aspect of sharing data between departments. This policy conforms to and augments Section VI - 440 of the County Procedures Manual.

F. PROCEDURE

1. Requests for individual or group access to any data that is not under the control of the requesting department will be submitted to the Custodial Department in writing by the requesting department (see Data Access Authorization form)

2. The request, combined with any details, will be forwarded to each affected control department for consideration by the Custodial Department.

3. The controlling department will determine whether an MOU exists or is required and will specify any requirements regarding restrictions for access. The authorization will be approved by the department head or designee.

3. Once approved by all affected controlling departments, the package will be filed in the Administrative Section of the Custodial Department for future reference.

4. The Custodial Department will implement access to the specified data within a reasonable amount of time following receipt of all approvals, unless special arrangements are made for a different schedule.

5. The Custodial Department will track and terminate individual, or group access based on the parameters defined in the Data Access Authorization form.

G. RESPONSIBILITIES

Users - responsible for reading, understanding, and adhering to this policy as well as Section VI-463 County Worker Acceptable Use Policy

Requesting Department - responsible for submitting requests for authorization.

Security Administrator- responsible for granting access to the data once all departments have been approved.

Controlling Department - responsible for completing the authorization for access to their data.

H. COMPLIANCE

The County reserves the right to monitor systems, audit use, and investigate potential violations of computer resources. Users will be held accountable for any breaches of policy, security, or confidentiality. Violations may result in disciplinary actions. Abuse or misconduct can be reported (by employees, supervisors, IT staff, the public, or others) to the appropriate authority for incident response and remedial action. Violations will be handled through the applicable union contracts, personnel rules, and County/State/Federal statutes. Depending on the nature and severity of the abuse, violations will be subject to appropriate disciplinary action, up to and including termination. Criminal or civil action may be initiated in appropriate instances.

I. EXEMPTIONS

None

J. AUTHORITY

County Procedures Manual Section VI-440
County Procedures Manual Section VI-410
County Procedures Manual Section VI-463

K. RELATED DOCUMENTS

Data Access Authorization form (click here)