Title VI – Information Services

Section 463 - County Worker Acceptable Use Policy

Latest Update: June 2024

A. OVERVIEW

The County of Santa Cruz (“County”) provides internet/intranet, data manipulation and storage systems, including computer equipment, software, storage media, network accounts, electronic mail, internet and intranet browsing, FTP and mobile devices (such as “smart phones”) and tablets, for County business purposes (collectively referred to as the “County’s information technology resources”). The County information technology resources are the property of the County.

B. PURPOSE

The purpose of this Policy is to: (1) protect the integrity of the data that resides within the County’s computer systems; (2) prevent data from being stored insecurely or accessed by unauthorized individuals; and (3) protect the County’s information technology resources from misuse or misappropriation.

C. SCOPE

This Policy applies to County employees, contractors, consultants, extra help employees (collectively referred to as “County workers”) and anyone accessing the County’s information technology resources.

D. POLICY

I. COUNTY COMPUTER SYSTEMS

A. **General use and ownership**

1. County Property. All data entered by County workers into the County computer systems or transmitted through the County’s computer systems shall be the property of the County.

2. Personal Use. County workers may use the County’s computer systems for incidental personal purposes, so long as such personal use does not interfere with the County worker’s job performance. Regardless of the intended purpose, none of data entered or transmitted through the County’s information technology resources shall be treated as private personal information but shall be treated as County property that can be accessed at any time without notice by authorized County personnel.

3. Departmental Guidelines. Individual departments may create guidelines concerning personal use and access to information technology resources, so

long as such guidelines are consistent with this Policy. In the absence of such policies, or in the event of a conflict, this Policy shall prevail.

4. System Monitoring. Authorized individuals within the County may monitor systems and audit use, equipment, and network traffic at any time.

5. The County provides active employees with computer accounts. The County will disable any account associated with an employee who is no longer in active status.

6. County workers are responsible for the security of their passwords and accounts. Passwords must be kept secure and may not be stored or "remembered" on any device external to the County network. All passwords shall meet or exceed the standards as outlined in County Procedures Manual Title VI, Section 466 – Password Policy.

B. **Unacceptable Use**

The following activities and use of County computer systems are prohibited. However, under no circumstances are County workers authorized to engage in any activity that is illegal under local, state, federal or international law while using or accessing County information technology resources.

Unacceptable uses include but are not limited to:

1. Violating copyright or other intellectual property laws or regulations, including installing "pirated" or other software products that are not licensed for use by the County or its individual departments.

2. Introducing malicious programs into the County information technology resources (e.g. viruses, worms, Trojan horses, malware).

3. Revealing account passwords or allowing others to use County worker's account.

4. Using County computer system to violate County policy or local, state, or federal laws regarding harassment or hostile workplace.

5. Effecting security breaches or disruptions of network communications, including any activities that adversely affect the ability of other people or systems to use the County computer systems, such as denial of service (DoS) attacks against another network host or individual user and all other forms of hacking.

6. Using any program/script/command or sending messages of any kind with the intent to compromise network or data security.

7. Providing information about County employees to parties outside of the County without authorization.

8. Stealing or misappropriating data or equipment.

9. Using County information technology resources for profit, commercial or political activity.

10. Removing or disabling any security device or software such as anti-virus and firewall applications that has been installed by County ISD.

II. MOBILE DEVICES

All County workers using mobile devices to access County computer systems must adhere to this Policy. County employment does not guarantee authorization to use mobile devices for access to County information technology resources. Such access is based on departmental approval and County business needs.

Mobile devices accessing County computer systems must use secure authentication and strong encryption methods managed and controlled by the County Information Services Department ("ISD").

Any County worker who uses a mobile device to access County computer systems must use such devices appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of the user access to County computer systems and immediate removal of all County data from the device.

Access Control and Security of Mobile Devices

1. ISD may deny access to County computer systems by mobile devices for any action deemed by ISD to be a risk to the County computer systems and users.

2. All users of personally owned mobile devices must enroll in the County Mobile Device Management system if they have access to confidential data (i.e. HIPIAA, payroll, personnel, or DOJ data). There will be a monthly charge to the department for each personal device enrolled in the Mobile Device Management system.

3. ISD reserves the right to dictate and enforce access methods to County networks, data, and email systems.

4. ISD reserves the right to manage security policies, network application and data access centrally where appropriate and necessary. Any attempt to contravene or bypass such security will be deemed an intrusion attempt and the device will be blocked, and the user account suspended.

5. County workers will follow all data removal procedures to permanently remove County specific data from personal devices once the data is no longer required. All County employees that are not in "active status" must ensure that all data and access via personal devices is removed and erased.

6. If a device is lost or stolen, the user must report the incident to the ISD Help Desk immediately. Appropriate steps will be taken to ensure that access to

County data is secured—including but not limited to password changes and account suspension along with remote removal of all County access and data from the device.

7. Employees who are approved for access using personal mobile devices are not eligible for support for device-specific hardware or software from ISD or other County sources. The employee is responsible for any necessary repairs or maintenance of employee's device.

8. ISD reserves the right to establish audit trails and logs to locate mobile devices attached to the County computer systems and such information may be used to investigate usage.

9. Mobile devices attached to the County computer system shall not be used in ways that are not designed or intended by the device manufacturer, including "jailbreaking", or "rooting" smartphones or other devices.

Employee Declaration

I have read and understand the *County Worker Acceptable Use Policy* and agree to comply with its rules and requirements. I understand that violations of this Policy may subject me to discipline up to and including dismissal. Further,

1. I acknowledge that all data entered or transmitted through the County's computer systems is not private and is the property of the County of Santa Cruz.

2. I will not to engage in any activities that violate the *County Worker Acceptable Use Policy*.

3. I will adhere to the guidelines in the *County Worker Acceptable Use Policy* for mobile device use and will apply security measures to protect data and access to County resources while using such devices.

_____ _____

Employee Signature Date