County of Santa Cruz

COUNTY ADMINISTRATIVE OFFICE

701 OCEAN STREET, SUITE 520, SANTA CRUZ, CA 95060-4073

(831) 454-2100 FAX: (831) 454-3420 TDD: (831) 454-2123

SUSAN MAURIELLO, J.D., COUNTY ADMINISTRATIVE OFFICER

June 8, 2009

AGENDA: June 16, 2009

Board of Supervisors
County of Santa Cruz
701 Ocean Street
Santa Cruz, California 95060

Procedures Manual Update

Dear Members of the Board:

Twice each year your Board considers recommended additions and modifications to the County Procedures Manual that is maintained and updated by the Clerk of the Board. Each of the recommended changes are provided in underline/strike-out format, followed by a clean copy of the modified procedure.

The Director of the Information Services Department recommends two new sections to the Procedures Manual. The Wireless Networking Policy sets forth policies for using wireless technologies at the County and assigns responsibilities for the deployment of wireless services and the administration of the wireless radio frequency spectrum in the County's network environment. The Data Access Policy outlines the rules and responsibility for sharing electronic information between departments. These sections will be added to *Title VI: Information Services: Telephone, Duplicating/Printing, and Data Processing.*

IT IS THEREFORE RECOMMENDED THAT YOUR BOARD approve the recommended revisions to the County Procedures Manual and direct the Clerk of the Board to make the identified changes.

Very truly yours,

Susan Mauriello
County Administrative Officer

cc: Each Department Head

14

Title IV: Telephone, Duplicating/Printing and Data Processing
Section 469: Data Access Policy

Summary
This policy outlines the rules and responsibility for sharing electronic information between departments at the County of Santa Cruz.

Goals
This policy is designed 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 professionally managed and secured.

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

Policy Statements

1. Ownership
Each piece of data kept in the County's data center or provided over the County's data network is controlled and maintained by a specific department. 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 center, or provided over the County's data network while it is on the network. Custodial responsibility also exists within DPW, HRA, HSA, and Parks over data in their data centers. 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 – 400, 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 implements part of Section VI – 440 of the County Procedures Manual.

Procedure

1. Requests for 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 attached form).

2. The request combined with any details will be forwarded to each affected

control department for consideration within three working days of the date the request was received by the Custodial Department.

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

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

Responsibilities

Users – responsible for reading, understanding and adhering to this policy.

Requesting Department – responsible for submitting requests for authorization.

ISD – responsible for granting access to the data once all departments have approved.

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

Compliance

The County reserves the right to 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 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.

Exemptions

Authority

County procedures manual section VI-400 "County ownership and access to computer data files and software"

County procedures manual section VI-410

Related Documents

• Access Authorization Form (attached)

Title IV: Telephone, Duplicating/Printing and Data Processing
Section 470: Wireless Networking Policy

1. Policy Purpose

The use of wireless networking provides a more versatile way to access the Internet and to use mobile devices, broadening the scope of mobile computing for County employees. This document sets forth the policies for using wireless technologies at the County of Santa Cruz and assigns responsibilities for the deployment of wireless services and the administration of the wireless radio frequency spectrum in the distributed County network environment.

2. DEFINITIONS

A. Wireless Network means local area network technology that uses radio frequency spectrum to connect computing devices to County Network and the Internet.

B. Access Point means electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a LAN, using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and are connected to the wired network, allowing access to the County network backbone.

C. Wireless Infrastructure means wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

D. Coverage means the geographical area where a baseline level of wireless connection service quality is attainable.

E. Client hardware/software means the electronic equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device to provide a LAN connection to a wireless network.

3. III. SCOPE

This policy applies to all authorized wireless network devices utilizing the County of Santa Cruz Network and all users of such devices. This includes services provided over wireless connections to all County locations to the County applications, resources and the Internet.

The County of Santa Cruz provides wireless networking connectivity for internal county use only and does not provide public wireless access to the internet or county resources for non-County users and devices (aka Public WiFi).

4. IV. POLICY

A. Wireless equipment and users must follow all County Information Technology policies as approved by the IS Policy Committee.

B. All acceptable use provisions of the County Internet Use Policy apply to wireless network services. Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless Network radio frequency spectrum is prohibited.

C. Only County owned and asseted devices (Workstations, laptops, printers and handhelds) are authorized and permitted to connect and use the County wireless network and related infrastructure within County coverage areas. Requested wireless access for vendors doing business with county departments will be reviewed upon request and determined on a case by case basis.

D. Wireless access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks. All wireless infrastructure must be reviewed by the Information Services Department prior to installation and connection to the County network backbone. All wireless devices must be checked for proper configuration by ISD or authorized support group prior to being placed into service.

E. Wireless access points shall require user authentication at the access point before granting access to County or Internet services. Wireless network interfaces and end-user devices shall support authentication to access wireless networks that allow connectivity to the Campus Network Backbone.

F. Wireless passwords and data must be encrypted. No application should rely on IP address based security or reusable clear text passwords. Other methods may be allowed but require the approval of the Information Services Department.

G. Wireless networks must be designed and deployed to avoid physical and logical interference between components of different network segments and other equipment.

H. Disconnect Authorization. Any wireless network on campus, which poses a security threat, may be disconnected from the County backbone network. If a serious security breach is in process, the Information Services Department or authorized support agency may disconnect the LAN immediately.