Title VII – Information Services

Section 465 – Remote Access Policy

Latest Update: June 2024

A. PURPOSE

The purpose of this policy is to define requirements for connecting to the County of Santa Cruz's network from outside the County network. The requirements are designed to minimize the potential exposure to the County network from damage that may result from unauthorized use of the County network resources. Damages include unauthorized access, loss of sensitive or confidential information, damage to public image and damage to critical County internal systems.

B. OVERVIEW

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the County of Santa Cruz and must be managed as such. Remote access controls are put in place to protect information resources by guarding against unauthorized use.

C. SCOPE

This policy applies to all County employees and agents with a County issued or approved computer or mobile devices used to connect to the County network. This includes remote access connections used to perform work on behalf of the County of Santa Cruz such as reading or sending email or viewing internal data or resources.

D. POLICY

1. All Remote access for County employees will be granted only upon written approval by from a Department Head or their designee. Vendor and outside agent access must be pre-approved by the requesting department and the Information Services Department prior to access.

2. Storage of confidential information on any non-County owned device is prohibited. Confidential information cannot be stored on any County-owned portable device without prior written approval from the Department Head or delegated authority. Approved storage of confidential information must be encrypted.

3. It is the responsibility of employees and contractors with remote access privileges that their remote access connection is given the same consideration as the user's on-site connection to the County network. Remote access to County resources should be commensurate with the tasks they are expected to perform. Suspected illegal use or tampering with remote access as in access gained through illegal or unapproved means will be reported to the County Administrative Officer or Director of Information Services Department by the applicable County IT support organizations or Department Computer Coordinators.

4. Remote access must be strictly controlled by the use of unique user credentials and must follow the County password policy and standard. Remote access passwords are to be used by only the individual to whom they were assigned and may not be shared.

5. All remote access by employees, agents and vendors must use the current approved software or appliance for access to the County network. All devices that are connected to the County network must have up-to-date protection software and current operating system security patches installed.

6. All remote access will be subjected to being monitored and periodic audits.

7. When an authorized employee terminates County employment or transfers to another County department, office or agency, all remote access services will be terminated. Remote access will have to be re-justified and re-established through the employee's new organization. County-provided hardware must be returned to the former organization. For contractors, vendors, non-County agencies, and other authorized non-employees' remote access shall be terminated when the contract, service, agreement, or other condition that justified the remote access is completed or terminated.

E. POLICY COMPLIANCE

Violators of this policy may be subjected to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.