Santa Cruz Consolidated
Emergency Communications Center
495 Upper Park Road
Santa Cruz, California 95065
(831) 471-1000 Fax (831) 471-1010

9-1-1 FIRE POLICE MEDICAL

Scotty A. Douglass
General Manager

COMMUNICATIONS TECHNICAL POLICY/PROCEDURE

Policy No.	**3083**	Date Issued:	December 2, 2003
Section:	3000 - Technical	Date Revised:	December 2, 2009

Accreditation Standards: CALEA 6.7.1, 6.8.5, 6.8.7

SUBJECT: COMPUTER SYSTEM SECURITY

APPROVED: _____
Scotty A. Douglass, General Manager

1.0 Purpose

This policy governs the security of the Authority computer systems. Computer system security is maintained through the administration of the Computer Aided Dispatch (CAD) Personnel (Security) File and by physical inspection of logins and passwords for the management and administrative network workstations.

1.1 The CAD Personnel File contains the names, personnel ID numbers, and passwords for authorized users of the CAD system.

1.2 The SCCECC Intranet Usage Log contains the computer IP addresses of the workstations that have accessed the internal website and shows foreign addresses that have attempted access.

1.3 Management and administrative network workstations are those computers that are assigned to personnel who work in a management or administrative capacity. It is typical that employees working in this capacity will have a workstation assigned for their exclusive use.

2.0 Administration

2.1 As with any computer system, proper administration and maintenance of the CAD Personnel File is necessary to maintain the integrity of the CAD system. This management becomes more important since the secure operation of mobile data computers in User agency vehicles depends upon

accurate security records. Personnel file maintenance includes, but is not limited to: additions, deletions, and modifications of user records; and audits of CAD security records.

2.2 To properly administer the CAD Personnel File, a single point of contact will be established to perform administration of the CAD Personnel file. This function shall be performed by Systems personnel as directed by the Systems Division Manager.

2.3 Only Systems personnel are authorized to perform the additions, modifications, and deletions of records in the CAD Personnel File and are the only personnel performing these duties except as described in Section 3, below.

2.4 The Systems Division Manager shall be provided a list of personnel from SCCECC and each User Agency for addition or deletion from the CAD Personnel file. This list shall contain the name, ID number, badge number and any other appropriate information, and be provided periodically and as often as necessary. The Systems Manager will assign the list to Systems personnel to reconcile the CAD Personnel File with the current agency personnel lists.

3.0 Accounts and Passwords

3.1 Management and administrative employees at SCCECC have a workstation assigned for their daily use. Each workstation is a member of the SCCECC Windows domain and requires authentication in the form of a user name and password. Employees are expected to secure their workstation by logging off or password-locking it whenever the computer is unattended. Management and administrative computers in the SCCECC Windows domain shall meet following password guidelines:

3.1.1 Passwords must contain a minimum of 5 characters. Users are encouraged to create passwords that are at least 8 characters.

3.1.2 It is recommended that passwords contain a mixture of alpha and numeric characters, and for the highest security the password should contain a mixture of upper and lower case alpha characters as well as numeric characters.

3.1.3 Passwords automatically expire after 90 days and the user is required to set a new password.

3.2 When establishing new accounts or auditing the CAD Personnel File, assigned Systems personnel shall use default passwords which contain a

mixture of alpha and numeric characters and which are at least 5 characters long. The CAD system is not case-sensitive and has no ability to force password resets or require specific password construction.

3.3 Information systems administered outside of SCCECC Systems (such as by the County of Santa Cruz) follow the administering agency's requirements for password construction, password reset and account administration.

3.3.1 Systems personnel at SCCECC work with other systems administrators to ensure external account lists are accurate and up-to-date, including notifying agencies when personnel terminate employment with SCCECC.

3.4 When personnel terminate employment with SCCECC, all user accounts including CAD accounts, Windows accounts and email accounts are deactivated by Systems staff as directed by the Systems Division Manager.

4.0 Exceptions

4.1 When an immediate, operational need arises requiring addition to the CAD Personnel file the following procedure will apply. Examples of immediate, operational need include, but are not limited to: adding a new officer to the CAD Personnel file so a unit may be logged-on; or, modifying a CAD Personnel file record to authorize an individual to perform a CAD function that s/he has the skill, responsibility, and an immediate need to perform said function.

4.2 SCCECC Supervisors and Lead Dispatchers have the authority and ability to add new personnel to the Personnel File. SCCECC Supervisors also have the ability to modify Personnel records and add additional functions to a user's security profile. Such modifications shall only be made when, in the opinion of the Supervisor, the modification is operationally urgent and cannot wait for Systems personnel.

4.3 Changes described in this section shall be documented via the Concern-Inquiry process in order to ensure continued proper management of the Personnel File by the Systems Division.

5.0 Audit

5.1 The Systems Division personnel assigned to manage the CAD personnel file will audit it quarterly to ensure the integrity of the CAD system. This

audit is accomplished by visual inspection of computer passwords as well as checking the CAD Security Violation file.

5.2 The Intranet Server Usage Log will be randomly inspected by the Systems Division Manager, no less than once per quarter, for unauthorized access based on workstation IP address.

5.3 Systems personnel as assigned by the Systems Division Manager will visually inspect each of the administrative office workstations on a quarterly basis. The employee inspecting these workstations will ensure a user login and password are being used by the employee assigned to that particular workstation.

5.4 Upon completion of the quarterly inspection, the Systems employee assigned to perform said inspection will document the results and forward them to the Systems Manager.