SANTA CRUZ REGIONAL 9-1-1
495 Upper Park Road, Santa Cruz, California 95065
831.471.1000 Fax 831.471.1010
Dennis Kidd, General Manager

COMMUNICATIONS TECHNICAL POLICY/PROCEDURE

Policy No.	**3083**	Date Issued:	December 2, 2003
Section:	3000 - Technical	Date Revised:	May 15, 2020

SUBJECT: WORKSTATION AND APPLICATION SECURITY

APPROVED: ______________________________
Dennis Kidd, General Manager

1.0 Purpose

This policy governs the security of the Authority computer systems. Computer system security is maintained through Active Directory (AD) security policy, AD Users and Groups, and application security including login and password management of enterprise systems.

2.0 Password Policy

2.1 Management and administrative employees at SCR9-1-1 have a workstation assigned for their daily use. Each workstation is a member of the Authority's 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 Windows domain shall meet the following password guidelines:

2.1.1 Passwords must contain a minimum of 8 characters. Users are encouraged to create longer passwords.

2.1.2 Passwords must contain a mixture of upper and lower case alpha characters, numeric characters, and special characters.

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

2.1.4 Failed login attempts will be logged. After 3 consecutive failed login attempts, the user's account shall be locked.

2.2 When establishing new accounts, assigned Systems personnel shall use default passwords which contain a mixture of alpha and numeric characters and which meet the password criteria outlined in section 2.1.

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

2.3.1 Systems personnel at SCR9-1-1 work with other systems administrators to ensure external account lists are accurate and up-to-date, including notifying external agencies when personnel terminate employment with SCR9-1-1.

2.4 The Authority Password Policy should match the FBI's Criminal Justice Information Services (CJIS) Security Policy language on password requirements. If the CJIS Security Policy guidelines and this policy do not agree, the stricter password rules shall prevail.

2.5 When personnel terminate employment with the Authority, all user accounts are deactivated by Systems staff utilizing the checklist maintained by the Systems Division

3.0 Application Security Administration

3.1 Enterprise accounts which access sensitive data, such as CAD, the recording server, or agency records systems shall be properly administered and maintained. Primary responsibility for management of enterprise accounts lies with the Systems Division.

3.1.1 To properly administer CAD Personnel security, a single point of contact will be established as the CAD Personnel administrator. This function shall be performed by Systems personnel as directed by the Systems Division Manager.

3.1.2 Systems personnel and Operations supervisors 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.

3.1.3 The Systems Division shall be provided a list of personnel from the Authority 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 CAD personnel administrator shall reconcile the CAD Personnel file with the current agency personnel lists.

3.1.4 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.

3.1.5Operations Supervisors have the ability to add new personnel and modify existing Personnel records.. Such modifications shall only be made when, in the opinion of the Supervisor, the modification is operationally urgent and cannot wait for Systems personnel.

3.1. 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 at least annually, or when personnel lists are provided, to ensure the integrity of the CAD system.

5.2 Upon completion of inspections, Systems personnel will document the results and forward them to the Systems Supervisor. Inspection audit results shall be retained for not less than one year.

5.3 The Authority may issue Mobile devices (laptops, tablets, smartphones). Such devices shall be audited at least quarterly to ensure virus definitions are up-to-date, operating system patches are applied, and the device is secured with a password.

5.3.1 If a device is lost or stolen, the user must report the incident to the Systems Division immediately. Appropriate steps will be taken to ensure that access to confidential data is secured—including but not limited to password changes and account suspension.