




Santa Cruz Consolidated Emergency Communications Center

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

Michael J. McDougall
General Manager

9-1-1 FIRE
POLICE
MEDICAL

COMMUNICATIONS TECHNICAL POLICY/PROCEDURE

Policy No. 3084	Date Issued: December 10, 2003
Section: 3000 – Technical	Date Revised:
Accreditation Standards: CALEA 6.8.6	
SUBJECT: BACKUP, USE, AND STORAGE OF COMPUTER FILES	
APPROVED: 	
Michael J. McDougall, General Manager	

1.0 Purpose

1.1 To establish a policy governing the backup, use, and storage of computer files, off-site storage of backup media, security of backup files and media, and destruction of backup files and media.

1.2 As technology progresses, the use of computers is becoming an integral part of the overall telecommunications process. Given this, it is essential that SCCECC institute policies for computer file and database backups.

2.0 Backup and Use of Computer Files

2.1 All server file systems (SCMRS) shall be backed up to tape automatically on a monthly basis by Systems Unit Personnel.

2.2 CAD system and event files shall be backed up to tape on a monthly basis by Systems Unit Personnel.

2.3 Closed CAD incident data from the SQL UDT shall be backed up to tape on a monthly basis by Systems Unit Personnel.

2.4 911 Server files shall be backed up to CD-R media on a monthly basis by Systems Unit Personnel.

2.5 File shares located on the server named UDT will be backed up to tape on a monthly basis by Systems Unit Personnel.

2.6 Intranet Web Files will be backed up to tape on a monthly basis by Systems Unit Personnel.

2.7 When the backups are complete, the Systems Unit employee performing said backups shall make an electronic entry into the SCCECC Backup Log located on the Center's File Server.

2.8 The SCCECC Backup Log shall capture the following information: Database or File being backed up, Media Type, Location Stored, Date of Backup and the first initial and last name of the employee performing the backup operation.

2.9 In the event of catastrophic data loss for any of the aforementioned systems, Systems Unit personnel shall be responsible for performing any and all restoration of those affected systems.

3.0 Onsite and Offsite Storage of Backup Media

3.1 Current month backup files and media shall be stored off-site in a fireproof safe in the SCCECC Tower Shelter. The Systems Unit employee storing the media shall fill out the *Tower Shelter Backup Media Check-In Log* located directly above the fireproof safe. This log captures the date, media type, label, responsible person, and initial of the employee performing this duty.

3.2 The previous month media will be removed from the fireproof safe and placed into the backup storage desk located in the Computer Room of the Center. Subsequently, the Systems Unit employee storing the media shall fill out the *SCCECC Computer Room Backup Media Check-In Log* located above the backup storage desk. This log captures the date, media type, label, responsible person, and initial of the employee performing this duty.

4.0 Security of Backup Files and Media

4.1 Only Systems Unit personnel shall have access to the locked fireproof safe containing the previous month backup data. The fireproof safe is located inside of the locked Tower Shelter which is also included inside a locked cyclone fence.

4.2 The backup media predating the previous month's backup shall be stored in the backup storage desk located inside the Computer Room which is in itself located inside the security of the Center.

5.0 Destruction of Backup Files and Media

5.1 Tapes will be reused when possible.

5.2 When backup media is no longer usable, it shall be physically destroyed by Systems Unit personnel so as to prevent access of confidential information by unauthorized persons.