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

Michael J. McDougall
General Manager

COMMUNICATIONS TECHNICAL POLICY/PROCEDURE

Policy No.	**3081**	Date Issued:	October 15, 2003
Section:	3000 - Technical	Date Revised:	
Accreditation Standards:	CALEA 6.8.3		

SUBJECT: INTRODUCTION OR ALTERATION OF COMPUTER FILES

APPROVED: _____
General Manager

1.0 Purpose

1.1 To establish a policy governing the introduction, removal, alteration, or downloading of computer files or programs.

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 the installation and maintenance of computer files and programs.

1.3 To minimize risk to computers and software programs, anti-virus software shall be installed on computers with Internet access.

2.0 Administration

2.1 At no time will any employee be allowed to add, delete, or alter any program file(s) on workstations or servers at SCCECC without the prior permission or under the direct supervision of Systems Unit personnel.

3.0 Downloaded Files

3.1 Management and Administrative Workstations with Internet access are protected with anti-virus protection. This protection will be configured ensure that any downloaded file will go be scanned for viruses.

3.2 Personnel that download files from the Internet or other insecure network location shall scan said files with the Symantec Norton Antivirus Software. In addition, personnel that are unsure about the integrity of a downloaded file shall immediately notify Systems Unit personnel who will inspect the file in question.

3.3 No employee will be allowed to download an executable file without first obtaining permission from Systems Unit personnel.

4.0 Inspection

4.1 All SCCECC workstations or servers will be inspected during the Annual Computer Software Audit performed by Systems Unit personnel and during the quarterly Computer Anti-virus Protection inspection. The Systems Unit employee performing these inspections will prepare and send a report based on their findings to the Systems Coordinator.