COUNTY OF SACRAMENTO
Inter-Department Correspondence

For the Agenda of: April 5, 2001

Date: March 14, 2001

To: Information Technology Policy Board Members

From: Ray Reis, Chair
Technology Review Group

Subject: Anti-Virus Software Policy

Recommendation:

Approve the Anti-Virus Software Policy defined in this document.

Background:

The County of Sacramento is at constant risk of losing employee productivity and data from the threat posed by computer viruses, trojan horses, worms and other software intended for malicious purposes. According to Trend Micro, Inc., there are more than 10,000 different viruses and 200 new ones identified every month.[1] During calendar year 2000, the County experienced nine documented cases of computer virus infection that resulted in loss of employee productivity.[2] In some cases, infections were exacerbated because of the lack of updated anti-virus software.

Discussion:

All computers capable of being virus protected will be virus protected. Departments must institute programs to acquire, install and maintain anti-virus software on all computers owned, leased, and/or operated by the County of Sacramento. Additionally, Departments must ascertain whether non-County computers that connect to the Sacramento County Wide Area Network (SCWAN) are equipped with anti-virus software before allowing such computers to connect

[1] http://www.antivirus.com/vinfo/vprimer.htm
[2] http://security/warroom/history.htm

to the SCWAN. The Chief Information Officer (CIO) may deny access to computers that do not have updated anti-virus software installed.

Anti-Virus Software Standards:

The County's "Technology Standards for Office Automation and E-Government Applications"[3] identifies anti-virus software suitable for use on County computers. County standard anti-virus software is preferred over other brands; however, any major brand of anti-virus software is better than none at all.

Anti-Virus Software Usage:

Anti-virus software will be installed on all computers that connect to the SCWAN. Definition files used by the software must be updated as soon as is practical after the manufacturer publishes a new release.

All software must be virus-checked prior to use on computers connected to the SCWAN. Virus-checks may be performed using a stand-alone or network-connected computer. Compressed files should be virus-checked both before and after being decompressed.

Anti-virus software must start automatically each time the computer is turned on. Users should be directed not to disable automatic virus scanning features.

Protecting Data:

For the purposes of protecting data and preventing the spread of viruses, users can:

- Virus check software and data files,
- Write protect software stored on workstations and removable storage disks in their possession, and
- Maintain back-up copies of data files.

Users are permitted to download and distribute data files from non-County computers provided:

- the non-County source has a track record of delivering virus-free files,
- license and copyright agreements are not violated, and
- all downloaded files are virus checked prior to use.

All storage media (i.e. disks) should be treated as if they contain viruses. Users are permitted to use removable storage disks provided that all disks are virus-checked prior to use. Users are encouraged to transfer files via the SCWAN instead of using removable storage disks to exchange data.

.

For additional protection, file integrity checking programs are recommended.

[3] http://www.co.sacramento.ca.us/depceo/itpb/aps/HWSW-Stds120700.html

Reporting Viruses:

Although users may not need assistance, users should be instructed to report computer virus incidents to their departmental Management Information System (MIS) staff. In the absence of MIS staff, viruses should be reported to the OCIT Help Desk. MIS staff should report virus incidents to the OCIT Help Desk and Virus Emergency Response Team.

Policy Changes:

Comments and suggestions affecting this document should be forwarded to the CIO for review. Before being implemented, changes to this document will be reviewed by the Technology Review Group (TRG) and must have the approval of both the CIO and the Information Technology Policy Board (ITPB). At least annually, the ITPB should review this document to determine whether additional changes are required.

Impact of Implementing the Recommendation:

If infected, a single computer can lead to network performance slow downs or even a complete denial of service. As a matter of good security practice, departmental staff have installed anti-virus software on most County computers. However, some computers do not have County-standard anti-virus software, do not have up-to-date anti-virus definitions, or do not have anti-virus software installed at all.

This policy is intended ensure that all County computers are protected against viruses.