5 FAH-2 H-860 ANTIVIRUS PROGRAM

(CT:TEL-19; 6-29-2007)
(Office of Origin: IRM/OPS/ITI/S)

5 FAH-2 H-861 POLICY

(CT:TEL-19; 6-29-2007)
(Uniform all agencies)

a. In accordance with 12 FAM 643.2-9, all systems connected to Department networks must be protected with *approved* virus detection and prevention programs. IRM/OPS/ITI/SI/IIB (Systems Integrity Division, Information Integrity Branch) provides antivirus software and documentation to all bureaus and field posts free of charge. The Setup and Installation Procedures Handbook*, included with the software,* answers procedural questions about installation. Contact IRM/OPS/ITI/SI/IIB at (202) 203-*5172* or visit the Virus Incidence Response Team Web site for more information.

b. *Employees and contract personnel may obtain antivirus software from the domestic bureau or post's systems office for home usage to prevent malicious code from migrating to the office environment. Home use antivirus software obtained in this manner may only be used while the employees and contract personnel are employed by the Department of State.* Diplomatic privilege and various host country custom laws may prohibit Foreign Service nationals (FSNs) or third country nationals (TCNs) from removing or installing Department of State procured antivirus software on privately owned PCs. *If not prohibited by host country law, copies of antivirus software may be requested for personal use through the antivirus program. See the* Virus Incidence Response Team's Cables Help Guide Web page. Licensing, reproduction, and distribution of antivirus software for domestic and post usage abroad are the responsibilities of the *a*ntivirus *p*rogram *s*taff, IRM/OPS/ITI/SI/IIB. *Information Programs Center (*IPC*)* personnel must install and update antivirus software on all computers maintained by the IPC (i.e., TEMPEST computers and non-TEMPEST classified computers within controlled access areas (CAAs)).

5 FAH-2 H-862 UNCLASSIFIED SYSTEMS

(CT:TEL-19; 6-29-2007)
(Uniform all agencies)

a. *DS/SI/CS (Office of Computer Security)* authorizes systems personnel to update virus signature files from the antivirus software vendor's Internet bulletin board or Web site via dial-up modem installed on an unclassified, stand-alone computer only. The computer may not be connected to or be a part of any LAN *including posts DIN or ODI LAN. The signature update files should be downloaded to a clean floppy diskette or CD-ROM that contains no sensitive information.* The standalone computer's hard drive must be scanned prior and subsequent to accessing the bulletin board or Web site. Scan the floppy diskette before use on any other U.S. Government computer. Use the clean floppy or CD-ROM to copy the signature update files to all other unclassified computers. Virus *signature* files and *software updates for Department approved antivirus applications* may also be downloaded directly from the Intranet IRM web pages.

b. At critical threat posts, *use the Guidance for Classified Systems in 5 FAH-2 H-863 below*.

5 FAH-2 H-863 CLASSIFIED SYSTEMS

(CT:TEL-19; 6-29-2007)
(Uniform all agencies)

Downloading of updated virus signature files from the Internet- or Internet-based bulletin boards for classified systems is **strictly prohibited**. *Virus signature files and software updates for Department approved antivirus applications* may be downloaded from the Intranet IRM Web pages for use on classified systems or for unclassified systems *at critical threat posts*. For all posts abroad, IRM/OPS/ITI/SI will send original program and updated antivirus signature files via classified pouch in the care of the information programs officer (IPO), information management officer (IMO) or a cleared U.S. citizen employee. The Department supplied CD-ROM disk or media containing antivirus software obtained from the Intranet IRM Web pages must be labeled with the highest classification of material processed, and once used, this media cannot be returned for unclassified use.

5 FAH-2 H-864 VIRUS INCIDENT REPORTING

(CT:TEL-19; 6-29-2007)
(Uniform all agencies)

If a virus is discovered, send *a report via e-mail to virus2@state.gov* and a courtesy copy to the Computer Emergency Readiness Team (CERT) at *CERT@state.gov, and an* official telegram or memorandum to the Department for IRM/OPS/ITI/SI/IIB and DS*/SI/CS/MIRCERT*. The report should include the following:

(1) Name of virus and occurrences;

(2) Location of virus (bureau, post or office);

(3) Origin of virus infection;

(4) Infected equipment type (stand-alone, LANs or network);

(5) Type of software used to eradicate the virus:

(a) *Specific application version (e.g., SAVCE 10.02.2021, ScanMail 6.2, etc.);*

(b) *Signature file installed (Date and/or sequence Number); and*

(c) *Scan Engine installed (Date and/or sequence Number)*;

(6) Losses incurred (defined as loss of equipment, software, or computer system downtime);

(7) Point of contact for follow-up support; and

(8) Remarks.

5 FAH-2 H-865 THROUGH H-869 UNASSIGNED