systems management

POLICY ON VIRUS PREVENTION, CONTROL, REPORTING, AND RECOVERY

1. **Purpose.** This operating procedure outlines agency policy to minimize damage from computer viruses and provides instructions for preventing, controlling, reporting, and recovering from computer viruses.

2. **Scope.** This operating procedure applies to all DCF employees and contractors.

3. **Explanation of the Term “Virus”.** A virus is a destructive computer software program written for the purpose of damaging a computer system by means of: destroying or modifying existing data files, destroying or modifying existing software files, consuming computer hard drive space making system processing difficult, or consuming computer memory making system processing difficult or impossible. This type of program attaches itself to other pieces of software, firmware or hardware. It is not easily detectable and can reproduce itself and be transferred from computer to computer on removable media, or transferred by uploading/downloading files over a LAN or other telecommunications connection.

4. **Responsibilities.**
   a. The Region IT Manager (or designee) is responsible for:
      1. Making sure that Department anti-virus software is properly loaded on each individual PC and servers and checking that the software is properly communicating with the central server that controls software updates to the virus signatures; [NOTE: Information on obtaining and using this type of software is available from the Office of Information Technology Services, the DCF Statewide Help Desk.]
      2. Ensuring that infected systems are isolated, cleaned, and monitored for re-infection;
      3. Tracking the virus to its source and determining if the virus has spread to other systems; and,
      4. Reporting to the DCF Information Security Manager in Information Technology Services (ITS) how the system was infected, the path the virus took, and an estimate of how much damage/cost the Department incurred.
   b. Production Services is responsible for working with the Region IT Manager and Data Security in the investigation of suspected viruses. Production Services is also responsible for working with the Region IT Manager and Data Security to isolate, clean, and monitor after virus detection.
   c. Data Security is responsible for:
      1. Working with all groups involved to facilitate the containment, eradication, and post infection monitoring of the system(s) involved;
(2) Collecting and tracking virus demographics from the DCF Statewide Help Desk files and Region IT Manager reports; and,

(3) Submitting any reports required by the State Agency for Enterprise Information Technology Services (AEIT) to comply with the State of Florida Information Resource Security Policies and Standards, Chapter 71A-1, Florida Administrative Code.

5. Procedures for Preventing Viruses.

a. New viruses are created almost daily. Companies that create virus-scanning software update their virus patterns (DAT/Signature) files on a regular basis. However, there will be occasions that staff may have a virus and the appropriate and up-to-date scanning software will not be able to detect the virus. To keep such instances at a minimum, it is imperative that the Department maintain current virus scanning software on all servers and PCs.

b. All DCF employees and contractors shall use the agency approved antivirus software to:

(1) Manually scan for viruses any removable media received from another person, whether from inside or outside of the person's immediate office area; and,

(2) Scan for viruses any files that are transferred onto their PC from any outside source.

c. All DCF employees and contractors that use remote connectivity to access the DCF Network must have antivirus software with updated virus patterns (DAT/Signature) on their personal computer.


a. DCF employees and contractors should report any suspicious or unexplained system behavior on any DCF owned or leased equipment to the appropriate Region IT Manager or the DCF Statewide Help Desk in the Office of Information Technology Services.

b. Once the DCF Statewide Help Desk or the Region IT Manager identifies the problem as a suspected virus, the user will be asked to isolate the machine by shutting it off and removing it from the Network by unplugging the Network Cable, and leaving it off until notified otherwise.

c. Information Technology resources are available to help the users and the Region IT Managers in isolating and eliminating viruses. Region IT Managers must report the disposition of virus investigations to Data Security for the benefit of users in all regions and Headquarters.

d. If staff notifies the Region IT Manager first, he or she will act as the coordinator in investigating and resolving the problem. If needed, Production Services, Data Security and/or the DCF Statewide Help Desk are available to assist the Region IT Manager in resolving the problem.

e. If staff notifies the DCF Statewide Help Desk first, Help Desk staff will assist the employee or contractor in identifying the problem, or coding it as a suspected virus if the problem cannot be identified. The DCF Statewide Help Desk will notify the Region IT Manager, who is responsible for virus troubleshooting and the Information Security Manager. The Region IT Manager will contact the user.

f. If the Region IT Manager determines that a virus is or may be present, the Information Security Manager will be notified and the DCF Statewide Help Desk ticket will be updated. Production Services will assist in identifying the virus, prescribe the remedy, and advise the user and the Region IT Manager with regard to clean-up and monitoring activities. The Region IT Manager will contact the
Information Security Manager to report the outcome of the investigation and update the helpdesk ticket.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

SCOTT STEWART
Assistant Secretary for Administration

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Corrected Florida Administrative Code reference in paragraph 4c(3).