

DEPARTMENT OF THE INTERIOR  
MINERALS MANAGEMENT SERVICE MANUAL

TRANSMITTAL SHEET

---

Release No. 201

March 25, 1992

SUBJECT: Administrative Series  
Part 375 Information Resources Management Program  
Chapter 20 Virus Policy

EXPLANATION OF MATERIAL TRANSMITTED:

This manual chapter prescribes policies, responsibilities,  
and procedures for detecting, preventing, and reporting viruses.

*Scott Sewell*

Director

---

FILING INSTRUCTIONS:

REMOVE:

None

INSERT:

<u>Part</u>	<u>Chapter</u>	<u>Pages</u>	<u>Release</u>
375	20	1-4	201

OPR: Information Resources Management Division  
Office of Administration  
Office of Management and Budget

DEPARTMENT OF THE INTERIOR  
**MINERALS MANAGEMENT SERVICE MANUAL**

Part 375 Information Resources  
Management Program

Administrative Series

Chapter 20 Virus Policy

375.20.1

1. Purpose. This chapter prescribes policies, responsibilities, and procedures for detecting, preventing, and reporting viruses.
2. Objective. The MMS virus policy is established for the protection of all automated information resources owned by or operated on behalf of the MMS to accomplish an Agency function.
3. Authority.
  - A. Public Law 100-235, The Computer Security Act of 1987.
  - B. Public Law 99-474, The Computer Fraud and Abuse Act of 1986.
  - C. OMB Circular A-130, Management of Federal Information Resources.
4. References.
  - A. Departmental Manual (375 DM 19 Information Resources Security Program and 441 DM 4 Personnel Suitability and Security Investigation Requirements).
  - B. MMSM 375.19 Automated Information Resources Security Program.
  - C. MMSM 386, Safeguarding of Records and Information.
5. Definition. A computer virus is a program that "infects" other programs by modifying them to include a copy of itself. Computer viruses can spread from one computer to another. They alter, manipulate, or destroy data and software programs. Computer viruses are usually transmitted by downloading infected programs over phone lines or by inserting a floppy disk containing an infected program into a computer. Depending on the author's motives, a program infected with a virus may cause damage immediately upon its execution or it may wait until a certain event has occurred, such as a particular date and time. The damage can vary widely and can be so extensive as to require the complete rebuilding of all system software and data. A computer virus is invisible to the human eye and is nearly always spread unknowingly by "friendly" hands.
6. Policy. It is the policy of the MMS that all information resources of the Bureau must be protected against loss of data or software programs by computer viruses.

OPR: Information Resources Management Division  
Office of Administration

Date: March 25, 1992 (Release No. 201)

DEPARTMENT OF THE INTERIOR  
**MINERALS MANAGEMENT SERVICE MANUAL**

Part 375 Information Resources  
Management Program

Administrative Series

Chapter 20 Virus Policy

375.20.7

7. Scope. This policy applies to all MMS employees. It also applies to contractor personnel providing information resources support to the MMS. The focus of the policy is on personal computers (PC's) and local area networks (LAN's). All MMS employees applies to both technical and non-technical computer users.

8. Responsibilities.

A. The Associate Director for Management and Budget is responsible for establishing policies and procedures for computer security practices commensurate with the value and sensitivity of the information resources.

B. The Chief of the Information Resources Management Division is responsible for implementing policy, coordinating compliance, and interpreting information resources security policies and instructions; developing MMS Automated Information System (AIS) Security Program policies and procedures; and reviewing of MMS implementation.

C. The Bureau AIS Security Administrator (BAISSA) is the individual within the MMS who has the responsibility for overall administration of the MMS Automated Information Resources Security Program as prescribed by 375 DM 19. The BAISSA will act as the focal point for ADP security matters concerning computer viruses.

D. The Installation AIS Security Officer (IAISSO) is the individual who serves as the point of contact for all ADP security matters, including computer viruses within the designated ADP installation.

E. Supervisors are responsible, to their immediate subordinate level, for ensuring compliance with this chapter; evaluating or designating an individual to evaluate new software; approving requests to transport and/or download over public or commercial networks executable programs; and ensuring that each subordinate is aware of his/her security responsibilities concerning computer viruses.

F. MMS employees will be vigilant to recognize the means by which viruses may enter MMS systems and take all reasonable precautions to prevent, protect against, and correct any infiltration. MMS employees are responsible for complying with information resources security policies and procedures of this chapter.

DEPARTMENT OF THE INTERIOR  
**MINERALS MANAGEMENT SERVICE MANUAL**

Part 375 Information Resources  
Management Program

Administrative Series

Chapter 20 Virus Policy

375.20.9

9. Procedures. In order to minimize the threat of viruses and protect against loss of data or software programs, MMS employees will take the following recommended actions. Actions apply to both end-user, technical and non-technical, or systems manager.

- A. Purchase software from reputable sources.
- B. Confirm that purchased software is in its original shrink wrap or sealed diskette container when received.
- C. Give new software to the immediate supervisor or person(s) designated by the immediate supervisor to evaluate for computer viruses before installing the software.
- D. Quarantine new software on an isolated computer, when possible, to test the software for computer viruses.
- E. Create backup copies of all system software and data once a month, where practical. Store backup copies for at least one year, when possible. Backups are especially important for LAN's. This will allow restoration of a system that has been contaminated by a "time released" virus. This procedure applies to the system manager or network administrator.
- F. Restrict access to programs and data on a "need to know" basis for MMS employees and contractors.
- G. Check programs regularly for length changes.
- H. Take a skeptical view of shared or free programs. They are the prime entry point for viruses.
- I. Remove software immediately if it exhibits symptoms of possible contamination.
- J. Transport diskettes containing executable programs between work and home only with the verbal approval of the supervisor. Data files, excluding proprietary data, may be transported without permission.
- K. Download executable programs over public or commercial networks only with the written approval of the immediate supervisor.
- L. Write-protect all program and system diskettes.
- M. Never boot hard disk systems from a floppy unless it is the original, write-protected, system master.

DEPARTMENT OF THE INTERIOR  
**MINERALS MANAGEMENT SERVICE MANUAL**

Part 375 Information Resources  
Management Program

Administrative Series

Chapter 20 Virus Policy

375.20.9N

- N. Never execute programs of unknown origin.
  - O. Never use network file servers as workstations.
  - P. Never add data or programs to system master diskettes.
  - Q. Report all known or suspected virus attacks to the supervisor or person(s) designated by the supervisor, and have the supervisor notify the IAISSO.
  - R. Purchase of anti-virus software is strongly recommended for PC's, especially if PC's are connected to a LAN.
  - S. Be suspicious of PC repairman using diagnostic software. Visually check to see that the diagnostic software is on an original write-protected diskette. If not, scan the diskette for viruses with virus scanning software. If that cannot be done, do not allow the diagnostic software to be used on the PC to be repaired.
10. Recognizing a Virus. To determine if a virus attack is taking place, consider the following questions:
- A. Do program loads take longer than normal?
  - B. Do disk accesses seem excessive for simple tasks?
  - C. Do unusual error messages occur with regularity?
  - D. Do access lights turn on for unreferenced devices?
  - E. Do I have less memory available than usual?
  - F. Do programs or files mysteriously disappear?
  - G. Do I notice a sudden reduction in disk space?
  - H. Have any executable files changed size?
  - I. Are unexplained hidden files present?

"Yes," answers to any of these questions could indicate that a virus is present in your system.