UNITED
NATIONS

ST

Secretariat

ST/IC/1990/8
16 January 1990

INFORMATION CIRCULAR

To: Members of the staff

From: The Assistant Secretary-General for General Services

Subject: VIRUS ALERT - HOW TO PREVENT MICROCOMPUTER VIRUSES

1. On the basis of problems encountered in several departments and offices, the Office Automation Service of the Electronic Services Division is issuing a virus alert. Personal computer (PC) users should be advised that a number of microcomputer viruses are now in circulation. These viruses represent a serious threat to the work of the Organization. All offices should be aware of the potential danger to personal computers, and should take steps to avoid a general infestation.

2. A virus is a special program, usually invisible to the PC user, which attaches itself to microcomputer programs and data. Having established itself in a PC, it then proceeds to damage programs, documents and data files. The virus may, for example, delete all files from the computer's hard disk. Alternatively, it may alter programs and data files in subtle ways, so that inaccuracies in data or documents result. Sometimes, viruses will degrade system performance so that the PC becomes unresponsive. Occasionally, a virus may display unusual messages, or cause intermittent hardware malfunctions. In any event, the results of a virus are malicious and destructive to the PC user.

3. Generally, viruses are not transmitted by copying data files and documents from one PC to another. Viruses are contracted by installing software which itself contains the virus. Even software which at first appears to be legitimate may be infected. Recently, there was a case where a supposedly reputable company distributed a program labelled AIDS Information, Introductory Diskette, Version 2.0, which appears to be professionally wrapped with diskettes and a licence agreement. However, if used on a PC, the user's system quickly becomes infected, and loss of valuable data will result.

4. Because of the problems associated with viruses, the Office Automation Service recommends that the following guidelines be followed by each PC user:

(a) The software source should be known. Software should be installed only if it has been obtained from the Office Automation Service, or if it is in the original sealed package obtained from a reputable dealer. Any software which arrives unsolicited in the mail should not be installed;

(b) Software should never be downloaded from a bulletin board. This is the most common way of infecting individual PCs. From there the infection spreads to entire work groups as the bulletin board software is copied;

(c) Software should not be copied from another PC. Another staff member's PC may have already been infected with a virus. Likewise, one used at home may be tainted. It is important to ensure that all copies of software packages residing on microcomputers owned by the Organization must have been purchased and loaded in accordance with copyright laws;

(d) Frequent back-ups should be made of files and documents. No matter how careful users may be, a virus could become resident on their PCs. If critical files and documents are backed up regularly, programs can be reloaded and data restored from back-up diskettes so that the amount of downtime suffered will be minimal;

(e) If a staff member suspects that his or her PC is infected, he or she should contact the Office Automation Service hotline (ext. 3-3157) immediately. The Office Automation Service has viral detection programs that can be run to determine if a machine has been infected. If so, a certain amount of diagnostic work will need to be done to correct the problem. Individual staff members SHOULD NOT attempt to repair the damage themselves.

5. If it is necessary to bring in a program from outside the Organization, the Office Automation Service is prepared to provide a quarantine service. Software left with the Office Automation Service will be run against software-checking programs on a special machine for that purpose. Upon return to the user, the Office Automation Service provides limited assurance that the software is virus-free.

6. Staff members should contact the Office Automation Service if they have questions or comments concerning the above guidelines or about viruses in general.
