23 SEP 1983

MEMORANDUM FOR: Chief, Management Liaison Staff,
Office of Communications

25X1 ATTENTION: [redacted]

25X1 FROM: [redacted]
Information Systems Security Group, OS

25X1 SUBJECT: Personal Computers [redacted]

1. It has recently come to the attention of the Office of Security, Information Systems Security Group (OS/ISSG), that Office of Communications (OC) components are purchasing Personal Computers (PC's) and individuals are also bringing in their own PC's and software for use within Agency facilities. This type of activity is contrary to existing Agency notices and ISSG policy. [redacted] 25X1

2. The purchasing of PC's and use of privately owned PC's, without coordination with ISSG, are in conflict with "ADP Contol Officer Bulletin Coordination Requirements Prior to the Acquisition of Personal Computers," ADP CO. Bulletin 83-003. This bulletin is derived from [redacted] 25X1

3. While ISSG policy does not disallow the use of PC's, we do require that components inform us of their plans to purchase PC's and submit to ISSG a memorandum that they have read and are in compliance with Policy Number 14 (attached). ISSG does not allow the use of employee-owned PC's in Agency facilities. Furthermore, ISSG security procedures require that once magnetic media (i.e., floppy disks) enters an Agency facility the media is not to be removed. [redacted] 25X1

4. In order to assist us in fulfilling our responsibilities, please inform ISSG of plans for complying with the attached policies and forward us a list of all PC's used by both foreign and domestic components. Additionally, please alert all OC components that purchases of PC's must be coordinated with ISSG, the Office of Data Processing, and the Office of Logistics. [redacted] 25X1

25X1 [redacted]

25X1 25X1 25X1

5. Please submit any questions to [redacted] extension [redacted] Your prompt attention to this matter will be appreciated. [redacted]

[redacted]

Attachments

cc: ODP/MS

ATTACHMENT 5

Policy Number 14 - Personal Computers* for Headquarters** Applications

1 The Office of Security feels strongly that the use of personal computers should be restricted to situations where the most stringent controls can be exercised. Their use poses formidable security problems and should be discouraged.

2. Experience to date clearly indicates that the use of unclassified word and data processing equipment in classified work areas creates a very real threat of contamination of the unclassified system. This is especially true of these small, "user friendly" computer systems. In fact, the smaller and more "friendly" the system, the greater the potential security risk. This contamination occurs in spite of conscientious efforts on the part of well intentioned individuals to prevent such occurrences. For this reason, all word and data processing accomplished in Headquarters work areas will be presumed to be classified. Thus, such processing will be handled and controlled accordingly.

POLICY

1. The Office of Security policy is to restrict the use of personal computers to only those applications which can be solidly justified for reasons such as efficiency and substantial cost savings, and where demonstrably robust security controls exist.

PROVISIONS

1. In those selected cases where sufficient management justification exists, the use of personal computers for the processing of Agency official information in a work-related capacity may be approved providing:

a. The use of personal computer equipment, in each case, is approved by the operating official or his designee, and the Office of Security.

---

* A personal computer is defined as one which (a) is easily transportable, (b) possesses limited software capabilities, and (c) requires few or no special devices for hook-up and operation.

** The Headquarters Building, the Agency training centers and Agency owned or leased facilities located in the Washington D.C. metropolitan area.

b. The personal computer equipment is TEMPEST approved, or otherwise controlled, in accordance with standards published by the Office of Communications.

c. The operating official or his designee creates, publishes, and promulgates written procedures designed to securely control the use of personal computers, and all associated magnetic media and printed output.

PROCEDURES

1. Procedures must be published and coordinated with, and concurrence received from, the Office of Security. This document must include strict procedures to:

a. Maintain positive segregation of classified processing from unclassified activities.

b. Provide for the use of unique identification labels for all magnetic media associated with and used for processing with personal computers.

c. Provide for the labeling of all personal computer generated output, including unclassified.

d. Provide for the definite segregation of unclassified personal computer printed output from classified program/project printed output.

e. Prevent the removal of all personal computer magnetic media from the facility. If data recorded on such magnetic media needs to be removed from Agency control, the data must be dumped to a factory fresh media, and the transferred data must be printed to verify that only the intended data is released.

f. Provide for the strict control of all magnetic media used for diagnostics and maintenance of personal computer systems.

g. Prevent the removal of personal computers from the Agency controlled area without proper sanitization and the written approval of the operating official, or his designee, and the Office of Security.

h. Prevent the relocation of personal computers within the program/project area without the written approval of the operating official. or his designee, and the Office of Security.

GENERAL

1. All personnel should be aware of the volatile/non-volatile memory characteristics of personal computers. Although most personal computers have volatile* memory, there are some personal computers which have non-volatile* memory. Also, some personal computers, whose basic design is categorized as volatile, employ a battery, a capacitator, or some other device to retain the data in memory for a period of time after a power failure, often for several days. Wherever possible, personal computers with volatile memory and no memory sustaining device should be used. Where such computers are not suitable, personal computers with non-volatile memory may be used provided memory is sanitized prior to power OFF at close of business in accordance with established procedures. In those instances where a memory sustaining device is employed, a positive disconnect feature must be employed to clear memory at close of business or when unattended.

2. Maintenance of personal computers also presents a problem which must be assessed as experience is gained. Thus, for the present, personal computers requiring maintenance must be repaired by staff or contractor personnel possessing an Agency Top Secret staff-type clearance.

3. Hardware components, software, and the computers themselves must be acquired through approved Agency sources only, and approved by the Office of Security.

4. Auxiliary storage media associated with personal computers, usually in the form of floppy disks and tape cassettes, will be destroyed in accordance with present regulations for non-soluble materials.

5. Personally owned personal computers will not be allowed in Agency classified working areas.

6. Each such approved personal computer system and published security procedures must be available for periodic security audits by the Information System Security Group, Office of Security.

- -

* Volatile memory does not retain the data recorded thereon after power OFF.

* Non-volatile memory does retain the data after power OFF, thus, the data is available upon restoration of power.

STAT