

23 AUGUST 2001



Communications and Information

SOFTWARE MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: 919 MSS/SCB (MSgt Carol S. Earnest)

Certified by: 919 SOW/CC
(Brig Gen Thomas M. Stogsdill)

Pages: 4

Distribution: F

This instruction establishes procedures and assigns responsibilities for using and managing the software program at the 919th Special Operations Wing (919 SOW). It implements Air Force Instruction 33-114, *Software Management*. It applies to all personnel assigned to the 919 SOW.

1. Purpose: This instruction implements local policies, procedures and requirements for all 919 SOW personnel in regards to the computer software program. All 919 SOW personnel are responsible for complying with procedures defined in AFI 33-114. Supervisors are responsible for enforcing the software program procedures and responsibilities as written. This instruction is to identify the responsibilities for management of all software used at the 919 SOW or at other locations under telecommute procedures IAW AFI 36-8002, *Telecommuting Guidelines For Air Force Reservists And Their Supervisors* and Wing Policy letters. Government computer resources are not to be used by personnel for activities such as playing games, producing unofficial products, using storage media for items of personal interest or amusement. All excess or unusable computer software or supplies are government property, and must be turned in or donated via appropriate channels, and are not to be given to individuals or organizations for personal use.

2. Responsibilities of All Software Users.

2.1. Software users must account for the use of all software issued to their offices. Software users are responsible for notifying their workgroup manager (WM) to collect all software licenses and installation disks not in their possession. Software users are:

2.1.1. Required to become familiar with the software license agreement for all software installed on their systems and used to accomplish their job.

2.1.2. Responsible for reporting all unauthorized or illegal software on their systems to their WM for resolution.

- 2.1.3. Responsible for reporting all software mailed directly to their office from AFRC for special programs; such as, FM, IN, SG, and DPM, to the WM immediately.
- 2.1.4. Required to receive a briefing on this instruction, upon assignment, from their appointed workgroup manager. In addition, all users are required to out process through the 919 MSS/SCB office prior to departure.
- 2.1.5. Responsible for ensuring all systems have the latest anti-virus software installed and programmed for a daily scan.
- 2.1.6. Not authorized to use shareware or public domain software prior to coordination with their WM for DAA approval.
- 2.1.7. Not authorized to install or remove any software application without first coordinating with their WM.
- 2.1.8. Not authorized to download and install freeware and shareware, for example screensavers, without coordination of their respective unit WM and 919 SOW DAA approvals.
- 2.1.9. Not authorized to make any illegal copies of copyrighted software. The user is responsible to ensure copyright infringement will not occur from installation on government systems.
- 2.1.10. Not authorized to install personally owned software on government systems.

3. Responsibilities of All Workgroup Managers.

- 3.1. Workgroup Managers (WMs) will collect, store and inventory all software license documentation and installation disks from their respective offices of responsibility. All inventoried software will be stored in the WM's library. WMs and supervisors of each section, will perform an annual software inventory beginning 1 January to be completed 15 March of each year. WMs and supervisors must work together to control software license documentation and installation of disks.
- 3.2. WMs are responsible for contacting Eglin's software manager before purchasing any software costing \$5,000.00 or more.
- 3.3. WMs are responsible for tracking software licenses and prevent the misuse of authorized software.
- 3.4. WMs will keep a list of all software utilized by their area of responsibility. A list of wing-authorized software is maintained in the 919 MSS/SCBN office.
- 3.5. WM must ensure software obtained from public venues (bulletin boards, shareware disks) or privately purchased are not installed and used on 919 SOW computer systems with out the 919 SOW DAA approval. The WM will certify the equipment's appropriateness and perform testing of software for malicious logic.
- 3.6. WMs are responsible for making sure all illegal software and games are removed from their computers within their area of responsibility. All new software must be accompanied by an AF Form 3215, **IT/NSS Requirements Document**, and routed through the 919 MSS/SCB office.

4. Software Installation.

- 4.1. Installation. The WM may authorize the user to install the software. The WM should be available to assist users with software installation problems. In cases where the acquisition contract specifies

vendor installation, the WM will coordinate with both the user and the vendor to ensure proper installation requirements are accomplished. The user will complete and forward vendor software registration cards to the software developer or contractor.

5. Software Management Accountability.

5.1. Software and accompanying documentation is accountable. Software (including shareware) with an acquisition cost of less than \$5,000 is accountable under the user's organization inventory control. A software package, with an acquisition cost of \$5,000 or greater with a life expectancy of two years or greater is accountable. If the life expectancy of a software package is unknown, the WM will treat it as accountable.

5.2. Desktop Management (DTM)/Tivoli will be used by the 919 SOW. This program will be installed and managed by the 96 Communication Group (96 CG). Each WM will download a listing from this program each month to identify all software currently installed and used by the 919 SOW. WMs will perform an audit of this listing to ensure all software programs are authorized. These lists will be compared to the approved master software list maintained in the 919 MSS/SCBN office. This program will include the following high level tasks: planning with sysadmins, installation of Tivoli software on all client PCs, establishment of roles that your sysadmins/workgroup managers will play (i.e., who gets inventory, remote control, and software distribution privileges), establishment of Tivoli administrator accounts for WMs and informal training for WMs.

6. Software Protection.

6.1. Each individual or shop chief must protect all software in use at their small computer processing location's. If a copyright violation is discovered, it must be reported to your WM immediately. The protection involves two phases and is explained below.

6.2. The first phase is that of copyright law restrictions. Federal copyright laws state each computer system has to have one master disk(s) and its documentation for each piece of commercial software that is used on the system. If the software you are using is "public domain" software, this means no copyright has been submitted against it and there are no restrictions for its use.

6.3. The second phase pertains to programs written by Air Force personnel. If the program is modified or written on duty, it does not belong to the individual who wrote it; it belongs to the Air Force.

6.4. Software protection for small computers is accomplished via floppy diskette protection. For software programs distributed via floppy diskette, the original copy is considered the "master" copy. Before using these programs, at least one, preferably two copies will be made of the program. This procedure is referred to as "backing up" your master program. After the back up is made, the master should be returned to the WM to be stored in a separate, secure location to protect it from use. The back-up copy becomes the working copy for day-to-day use.

7. Excesses.

7.1. Sections with excess software should contact your WM for specific instructions. If determined to be unusable, disks containing software programs may be destroyed or reformatted for reuse, and the manuals disposed. WMs may have a need for this software in another section.

8. Viruses.

8.1. A computer virus is a program, which can destroy or erase data or lock up the system. To minimize the risks associated with passing or receiving infections, the following guidelines should be observed. Do not:

8.1.1. Introduce, download and/or play unauthorized computer games.

8.1.2. Introduce shareware or freeware unless approved in writing IAW AFI 33-114 and its supplements. Contact your WM.

8.1.3. Copy software beyond the limits of licensed agreements.

8.1.4. Design, develop, and implement software outside of authorized program management channels.

9. Fraud, Waste and Abuse of Computer Resources.

9.1. The policy concerning the use of computer resources assigned to Air Force activity states all government acquired and their support materials are solely for the authorized use of the Air Force and are subject to monitoring. Any abuse of these resources is prohibited and failure to comply with this policy may result in disciplinary action.

9.2. No person will use government computer resources for activities such as playing games, producing unofficial products, using storage media for items of personal interest or amusement. All excess or unusable computer supplies are still government property, and must be turned in or donated via appropriate channels, and are not to be given to individuals or organizations for personal use.

9.3. No person will temporarily alter, damage, destroy, or attempt to damage or destroy government computer resources.

9.4. Any software developed or modified using government resources are the property of the government and may be used for official business.

9.5. Beware of public domain software; it is not tested and documented with the thoroughness associated with commercially developed software.

THOMAS M. STOGSDILL, BRIG GEN, USAFR
Commander