

**BY ORDER OF THE COMMANDER
315TH AIRLIFT WING**

**315TH AIRLIFT WING INSTRUCTION
33-114**



27 AUGUST 2012

Communications and Information

***SOFTWARE LICENSE MANAGEMENT
PROGRAM***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-publishing website at www.e-publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 315 FSS/SCOS

Certified by: 315 FSS/SCO
(Colonel William R. Fingar)

Supersedes: 315AWI33-114, 7 April 2009

Pages: 6

This instruction implements Air Force Instruction (AFI) 33-114, *Software Management*, Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*, T.O 00-33A-1001 *Methods and Procedures, General Communication's Activities Management Procedures and Practice Requirements*, and AFI 33-200, *Information Assurance (IA) Management*. It explains how to manage accountability for computer software licenses, mandates specific roles, responsibilities and processes for software license accountability to meet requirements of Section 1(c) of Executive Order (EO) 13103, *Computer Software Piracy*. It incorporates enterprise license and Standard Desktop Configuration (SDC) considerations, Communications Support Center (CSC) personnel responsibilities, and specific requirements for placing software on PCs and computer network systems. It applies to all 315 AW organizations.

Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims>.

SUMMARY OF CHANGES

This instruction has been substantially revised and must be completely reviewed.

1. Roles and Responsibilities

1.1. 315 AW/CC Responsibilities.

1.1.1. As the 315th AW responsible official for software license management, designate a primary and alternate Wing Software License Manager (WSLM) to manage the wing Software License Management Program.

1.1.2. Forward WSLM appointment memorandum to the command software license manager (HQ AFRC/A6XR).

1.2. Wing-level Software License Manager Responsibilities.

1.2.1. The WSLM is responsible for management of the wing level Software Management Program.

1.2.1.1. Establish a process to track all software to ensure effective software control and accountability to include deployment/unit type code (UTC) requirements. Limit access to minimize fraud, waste and abuse.

1.2.1.1.1. Coordinate with and obtain approval from host communications unit or servicing network operations center prior to implementing any software.

1.2.1.1.2. Establish a process to track software licenses.

1.2.1.1.3. Establish documentation procedures for the annual inventory of software and licenses as required by E.O.13103.

1.2.2. In accordance with AFI 33-114 para 9.9.2, Software Management, dispose of old versions of COTS software according to licensing agreements. Upgrades from the original software source are normally considered a continuation of the original license, not an additional or new license.

1.2.3. Certify the completion of an annual inventory of all unit computer software and licenses.

1.3. CSC Responsibilities.

1.3.1. Maintain a current inventory of the COTS software controlled by organizations to include: software version, unit assigned location (bldg/room), system number, system name, and system serial number. Inventory documentation must be updated when:

1.3.1.1. Obsolete software is returned to the WSLM for destruction or redistribution

1.3.1.2. Software is installed on a different system

1.3.1.3. Software is transferred to another account

1.3.2. Create a "memo for record" for software transferred to another unit or returned to WSLM.

1.3.3. Perform an annual software inventory by the first Friday in June, or when a new CSC POC is assigned specific group level duties. Accomplish certification by forwarding a signed compliance memorandum, along with software inventory (Attachment 2).

1.4. System User responsibilities:

1.4.1. In accordance with AFI 33-100, users will not install and use copies of government-owned software on a home computer unless the software license explicitly

allows users to do so and the installation CSO has authorized such use. This action may be a violation of The Copyright Act, rendering the individual user accountable and liable.

1.4.2. Do not install software or hardware on an IS without coordination with the IAO. The IAO is responsible for the proper coordination and implementation through IA channels.

2. Software Purchases.

2.1. CSC Personnel will:

2.1.1. Identify/justify need for software purchase and creates trouble ticket (REMEDY), to include required information regarding purchase:

2.1.1.1. Details of software requested (name, version, and cost). Attach information as needed regarding local vendor.

2.1.1.2. Justification for desired purchase. What, why, where software will be used, impact on mission.

2.2. WSLM will:

2.2.1. Upon request notification, validate requirements.

2.2.2. Request local approval for purchase. Approval is based on host unit and HQ AMC software approval process requirements. Refer to the AF approved transitional list (<https://afkm.wpafb.af.mil/ASPs/DocMan/DOCMain.asp?Tab=0&FolderID=OO-SC-IA-01-31-14-2&Filter=OO-SC-IA-01>) to determine approval status. Requests for software versions not listed will be forwarded to HQ for testing and inclusion on approved software listing - process may require a single purchase of the software being submitted to HQ AMC for testing. Once added to list, future purchase of the software edition will be eligible for local approval.

2.2.3. Following approval, forwards requirement to ECO for purchasing.

2.2.4. Track IT/NSS request until the purchase is complete.

2.2.5. Receive the actual software and copies of purchase documentation to ensure inclusion in wing software management program inventory.

2.2.6. Release to CSC personnel.

2.3. IT GPC Approving Authority. All software purchased in this wing must be purchased using the Information Technology Government Purchase Card. The IT GPC Approving Authority will notify the ECO when the appropriate funds have been transferred to the IT GPC Account and the purchase can be made.

3. Equipment Control Officer (ECO) will purchase all requested COTS using government purchase card. Purchases will be delivered to the ECO. Actual Software and copies of purchase documentation will be forwarded to the WSLM.

WILLIAM R. FINGAR, Colonel, USAFR
Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

The Copyright Act

The Information Technology Management Reform Act (Division E of Public Law 104-106)

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 33-100, *User Responsibilities and Guidance for Information Systems*

AFI 33-114, *Software Management*

Abbreviations and Acronyms

AFI—Air Force Instruction

C4—Command, Control, Communications, and Computers

COMPUSEC—Computer Security

COTS—Commercial Off-The-Shelf

CSC—Communications Support Center

CSO—Communications and Information Systems Officer

ECO—Equipment Control Officer

GPC—Government Purchase Card

IS—Information System

IT—Information Technology

IAO—Information Assurance Officer

MAJCOM—Major Command

PWRR—Project, Workflow, Requirements, and Resource Manager

SDC—Standard Desktop Configuration

WSLM—Wing-level Software License Manager

Terms

Certification—For purposes of this instruction, the act of determining that software performs without defects and viruses, and does what the supporting documentation says it will do in accordance with any specified acceptance criteria.

Command, Control, Communications, and Computer (C4) Systems—Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, across the range of military operations. Also called "communications and information systems."

Communications and Information Systems Officer (CSO)—Identifies the supporting CSO at all levels. At base level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities, the base CSO. Tenant organizations may also have CSOs. At MAJCOM, and other activities responsible for large quantities of communications and information assets, it is the person designated by the commander as responsible for overall management of communications and information assets budgeted and funded by the MAJCOM or activity. The CSO function, when under the base communications unit, uses the office symbol “SC” that expands to three or four digits to identify specific functional areas.

Computer Security (COMPUSEC)—1. The protection resulting from all measures to deny unauthorized access to exploitation of friendly computer systems. 2. Measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

Copyright—Without a license that specifies otherwise, the purchaser’s use of software is restricted to making an archival copy and installing the computer program onto a single computer, in accordance with the Copyright Act of 1976. Do not reproduce or use copyrighted software in any other manner.

Enterprise License—Allows the purchasing organization to use a specific COTS software program across the organization for a set price. This is usually a more cost effective acquisition strategy than purchasing individual copies for widely used software. The user should refer to the contract terms and conditions to determine if the enterprise license is limited or unlimited. Either the Air Force Enterprise Software License Program or DoD ESI should be considered for commonly used software.

Enterprise Software Agreement (ESA)—Agreements, such as contracts or blanket purchase agreements, by which organizations acquire, software or software maintenance under specified terms and conditions.

Requirement—A need for a new or improved information processing capability that, when satisfied, increases the probability of operational mission success or decreased the cost of mission support.

Reuse—The process of developing or supporting a software intensive system using existing software assets.

