
State of California
Office of the State Chief Information Officer
Software Management Plan
Guidelines

Revised November 2009

Section 1

INTRODUCTION TO SOFTWARE MANAGEMENT PLANNING

1.0 Overview

The State Administrative Manual (SAM) Section 4846 – 4846.2 describes the state's policy regarding software management. Specifically, Section 4846 states as follows:

Each agency shall establish and maintain appropriate computer software management practices and ensure that computer software they use and/or have purchased with state funds is legally procured and is used in compliance with licenses, contract terms, and applicable copyright laws. Each agency shall develop and implement policies and procedures to ensure that all staff understand and adhere to proper software management policies.

Software piracy refers to the installation or use of unlicensed or unauthorized copies of software. This can occur through using one licensed copy to install a program on multiple computers or taking advantage of software upgrade offers without having a legal copy of the version to be upgraded. Piracy includes having the number of simultaneous users on the network exceeding the number of available client licenses for a networked program, unauthorized downloading of software from the Internet, or illegally duplicating and using copyrighted materials such as counterfeit copies of CD's, diskettes and related manuals and materials.

The Office of the State Chief Information Officer (OCIO) permits the use of Open Source Software (OSS). Consistent with other software, use of OSS is subject to the software management licensing and security practices included in e SAM, Sections 4846, 4846.1, 5310–Item 2 and Item 5, Subsection (f), and 5345.1.

1.1 Roles and Responsibilities

Office of the State Chief Information Officer:

The OCIO is the principal government department responsible for improving executive agency practices regarding the acquisition and use of computer software, monitoring and eliminating the use of unauthorized computer software. The OCIO will utilize appropriate oversight mechanisms to monitor and audit expenditures by state agencies to foster state agency compliance with the policies set forth in SAM Section 4846 and with established policies and guidelines.

Department of General Services:

The Department of General Services will develop appropriate language for inclusion in State contracts to require compliance with software licenses and applicable copyright laws when State funds are used to acquire, operate, or maintain computer software.

State Agencies:

State agencies shall develop, implement, and maintain specific plans, procedures, and processes to ensure compliance with the established requirements. State contractors and recipients of state grants and state loan guarantee assistance shall have appropriate systems and controls in place to ensure state funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws. Each state agency shall designate an appropriate position or unit to be responsible for ensuring compliance. Each state agency's compliance program shall be documented with sufficient specificity to meet the audit requirements by its internal auditors and Information Security Officer.

1.2 Introduction to the Guidelines

These guidelines have been issued to assist state agencies in developing or continually administering a software management program to prevent software piracy and promote good software management practices. The guidelines are also intended to assist agencies in preparing a Software Management Plan (SMP) as required by SAM Section 4846.1.

The absence of an effective SMP exposes an organization to a variety of tangible and intangible risks including:

- damage to the organization's reputation
- fines from civil damages for copyright infringement
- denial of product support or warranty service
- the possibility of civil and criminal charges against the directors and managers of an organization found in violation of copyright

The benefits of an effective software management program are many. These include:

- the ability to determine actual software costs
- the ability to obtain technical support for installed software products
- access to information relating to upgrade issues
- the ability to plan future expenditures more accurately
- the knowledge that licensing of installed software is accurately documented by the current software inventory and listed on the agency's supported software list.

1.3 Practices That Support Good Software Management

To manage software properly, the following practices should be followed:

- Have and maintain a comprehensive inventory of all installed software including microcomputers, mid-range, and mainframe environments and maintain complete and accurate records of all licenses, certifications and software purchase transactions, storing these in a secure repository.
- Periodically review installed software and accompanying licenses to ensure only legal and supported software are in use and to ensure ongoing compliance with the Software Management Policy.

- Be familiar with the U.S. Copyright Act found in Title 17 of the U.S. code in order to understand the consequences of infringement of copyright laws including the penalties and liabilities for damages.
- Be familiar with the licensing agreements for each individual software vendor in order to understand the limitations, such as transferring of licenses, expiration of licenses, when support ends for licenses, when upgrades will be needed, requirements for patches, whether or not software can be installed on home computers, how to terminate a license, etc.
- Have and maintain a software management program and train management and staff on the policies and procedures associated with that program to ensure the use of best practices in software management and compliance with the policy.
- Have and maintain a list of supported software to guide what new software will be approved for purchase and what current software should be retained on the desktops, servers and other processing devices.
- Remove all unlicensed software and software not on the supported software list, software no longer in use from individual computers, and non-authorized software to make sure all software is legal and supported and to free the hard drive space of unused software.
- Purchase software only in the name of the state agency; not in individuals' names.
- To the extent that the use of freeware and OSS is allowed by policy within the department, make sure that such usage is approved on a case by case basis and that appropriate controls and processes are in place to ensure that software is used in accordance with any conditions or agreements prescribed by the manufacturer.
- To the extent that software purchased by end users is allowed by policy to be installed on a department's computers, make sure that such usage is approved on a case by case basis, that appropriate controls and processes are in place to ensure that proper licensing is secured, and that the software is used in accordance with the licensing agreements.
- Do not allow state licensed software to be installed on non-state equipment except as specified in a service contract or other legal document that requires the parties to adhere to the agency's Software Management Policy.
- Transfer and dispose of software according to license agreements to ensure proper disposition. Wipe or scrub hard drives of all software when computer devices are recycled or salvaged as necessary to comply with the terms of the licensing agreement and to protect any confidential or sensitive data.
- Require that software be acquired through a formal acquisition process to ensure proper approvals are obtained, and that proper stock receipt, registration and inventory records are created and maintained.

Section 2

STEPS FOR PREPARATION OF SOFTWARE MANAGEMENT PLANS

2.0 Overview

The Software Management Policy requires the identification of the software management roles and responsibilities within the organization and the submittal of a supported software list by each department. Most agencies have designated software management roles and responsibilities to staff within their organization. The same person may perform multiple roles; however, one individual needs to be designated as ultimately responsible for each specific software management task. In addition, agencies should have and maintain a list of approved and supported software. The objective of the following guidelines is to assist state agencies in developing their Software Management Plans.

To prepare for developing the plan, state agencies should:

2.1 Have A Software Management Team

As resources allow, have a Software Management Team that will be responsible for developing and implementing the software management program as well as preparing the SMP. The team should consist of:

- A Software Assets Manager or other job title whose roles and responsibilities are:
 - Understanding general licensing procedures and specific requirements of software, including open source, used within the organization and knowing the particular limitations of the agreements.
 - Maintaining a list of approved software for use in the acquisition process and the process of identifying unlicensed and unsupported software.
 - Maintaining a baseline inventory of all software residing within the agency to serve as the foundation for the software management program.
 - Performing ongoing inventories for asset management and compliance purposes.
 - Selecting and securing an automated tool to be used in conducting the baseline and ongoing inventories, should the state agency decide to acquire/use such a tool.
 - Making sure that all software is registered, and that the records of licenses and renewals are properly maintained.
 - Ensuring all unlicensed software is removed from computers, servers and other processing devices.
 - Ensuring there is a secure repository for all software licenses and software media to prevent loss, misuse and theft.
 - Ensuring that proper checkout procedures are developed and followed for loading software onto the agency's computers.

- Maintaining a software log to record when software is checked out of the repository, who checked out the software, why the software was required, and when the software is returned to the repository.
- Ensuring that proper education on software management practices is available within the organization and that training through new employee orientations, etc., is administered to all levels of staff including users, acquisition support, technical, management and executives. Staff need to be aware of copyrights protecting computer software and the policies and procedures adopted by the agency to honor those copyrights.
- Ensuring the required Software Management Plan and certifications are developed and maintained according to the schedule outlined in the State Information Management Manual Section 05A.
- Monitoring the use of software on state owned desktops and mobile computers, which includes those used in the home environment to accomplish state work.
- Ensuring corrective action is taken in terms of correcting any license agreement breaches and ensuring the policy and procedural flows that led to failures of compliance are modified to prevent further problems.
- An Acquisition Manager or other job title whose roles and responsibilities are:
 - Understanding general licensing procedures and specific requirements of software used within the organization including the limitations of the agreements.
 - Ensuring that proper software procurement practices are in place and followed.
 - Ensuring proper education of acquisition staff in software procurement practices.
 - Ensuring language is included in state contracts requiring vendors to certify that they have appropriate systems and controls in place to ensure that state funds are not used to acquire, operate or maintain computer software in a manner that does not comply with applicable copyrights.
- A Desktop and Mobile Computing Coordinator whose roles and responsibilities are:
 - Reviewing software acquisition requests that are being purchased through the Desktop and Mobile Computing Policy to ensure purchases are in concert with the agency's supported software standards.
 - Reviewing exception requests for purchases of software not on the agency's supported list and making recommendations to the Software Manager as to the appropriateness of these purchases and the addition of the software items to the supported software list.
- A Software Administrator or other job title, for mainframe and mid-range computing systems, whose roles and responsibilities are to manage software assets: NOTE: This is also desirable in network installations and desktop and mobile computing.
 - Ensuring proper licensing on installed hardware is in accordance with contractual requirements.

- Negotiating the terms and conditions of software usage with appropriate vendors, departmental procurement staff, and/or the Department of General Services.
- Managing the physical inventory of software orders and maintaining a software inventory database of departmental software assets.
- Monitoring all installed and distributed copies to ensure software copyright protection.
- Acquiring new software, upgrades and fixes as necessary.
- Keeping abreast of all new and existing licensing requirements.
- Internal Auditors whose roles and responsibilities are:
 - Performing internal audits as necessary to evaluate the existence and effectiveness of the SMP.
 - Taking steps to verify that recommended corrective actions are taken and ensuring that the appropriate management is notified when violations occur.

2.2 Have And Maintain A Methodology To Conduct A Full Software Inventory

Each state agency must regularly conduct a full software inventory applying the practices outlined above. State agencies are advised to research alternatives for conducting a full inventory of all software residing on the agency's information technology systems. Alternatives can include acquiring an automated tool, preparing an inventory through manual procedures, or contracting for an inventory service.

- Automated tools are available that can inventory computer software through a variety of techniques. In selecting an automated tool, consider:
 - Ease of use, requiring minimal training for IT staff
 - Accuracy
 - Flexibility
 - Completeness
 - Extensibility, enabling the tool to be used on multiple platforms
- A manual inventory can be conducted by individually accessing each computer and listing the software on each machine.
- Contract services are available for conducting a software inventory as well as providing additional services such as training, auditing, and developing software management plans.

2.3 Have And Maintain A List Of Supported Software

To standardize on the purchase and usage of software for desktops and networks, have and maintain a list of supported software. The list will facilitate procurement as well as assist when auditing for software management compliance.

For a supported software list:

- Identify with specificity the software supported within the organization. The list should contain the following information:
 - Class of software (operating system, word processor, spreadsheet, database, e-mail, utilities, graphics, network)
 - Name and version of software (Office 2007, Adobe Acrobat 9, Windows XP Service Pack 3, McAfee, etc.).
 - Sub-class of software (OS390, Windows, Word, Excel, Access, ADABAS, IDMS, DB2, Groupwise, Outlook, WinZip, Norton, Corel Draw, Novell, Unix)
 - Type of license (enterprise or standalone),
 - Appropriate user base (clerical support, technical, management, executive)

2.4 Have And Maintain A Software Procurement Process

It is essential that the purchasing of software be a standard procedure consistent with the acquisition of other critical department assets. All software purchases should proceed through the state agency's normal purchasing process, requiring requisitions and management approval.

Components of a software procurement program and process that will promote proper software acquisition may include:

- Educating and training procurement staff on software licensing and copyright laws.
- Centralizing all software purchases to promote adherence to standardized software procurement processes.
- Establishing a signature process to ensure responsible parties are aware of and approve each software acquisition.
- Requiring that all software purchases be accompanied by proper licenses and receipts, evidencing legal acquisition and use.
- Requiring that all software purchases be made through reputable, authorized resellers to prevent purchasing counterfeit programs.
- Obtaining licenses and receipts for each purchase.
- Ensuring that purchased software is registered with the manufacturer, if required.
- Ensuring software cannot be downloaded and purchased from the Internet without approval.
- Ensuring that purchased software is listed on a comprehensive software log.

2.5 Have And Maintain Record Keeping Standards

Maintaining complete and accurate records is essential for a good software management program. To ensure that a software compliance program is ultimately successful, have and maintain good record keeping standards to assist internal auditors and other audit officers in conducting a comprehensive examination of software compliance.

Proper record keeping should include:

- Maintaining software purchase records (purchase order, invoices, receipts, copies of cancelled checks, if appropriate).
- Maintaining a repository of software media, documentation, product licenses, license agreements, manuals, and registration cards. Store software media, licenses and registration cards in a secure area to prevent theft, loss or misuse.
- Maintaining a software log including product and version, publisher, software serial number purchase date, user name, user location, hardware serial number and comments.
- Maintaining records of staff who have attended training in software management practices or have been introduced to software copyright requirements and appropriate software usage through other educational opportunities such as employee orientation.

Section 3

SOFTWARE MANAGEMENT PLAN

3.0 Overview

Software management is an important component of a State agency's overall resource and compliance management process. The Software Management Plan (SMP) enables agencies to lay out the framework for a software management program to ensure that all State agencies meet the requirements of the California Software Management Policy as stated in SAM Sections 4846 – 4846.2. These guidelines have been prepared to assist state agencies in developing the required SMP. To the extent that agencies have existing documents that have been developed through the administration of the Desktop and Mobile Computing Policy or other internal department efforts and that these documents will meet the requirements of the SMP, they can be submitted in lieu of creating new documentation.

The SMP should include the following information to indicate how the state agency plans to address the required software management program activities to come in full compliance with the state IT policy or how the state agency is already accomplishing these activities and will continue with the administration of a software management program.

3.1 Baseline Inventory Methodology

It is essential that a baseline inventory be conducted in order to know what software exists within an agency so that it can be properly managed. An inventory consists of determining all software physically residing on an agency's computers and inventorying all original licenses for the software.

The SMP must address:

- Who is involved in conducting the inventory (organization/classification);
- What inventory methodology is used (e.g. automated tools, manual processes, contract services);
- How the inventory process is organized;
- What information is gathered;
- How the information is reported (e.g. form, summary report);
- Who receives the inventory information (software management team members, CIO, agency director); and
- The baseline inventory completion date.

3.2 Unlicensed/Unauthorized Software Identification Methodology

The identification of unlicensed and unauthorized software is accomplished by: 1) comparing the results of the physical inventory with the license agreements, and 2) comparing the results of the physical inventory to the list of software authorized by the organization.

The SMP must address:

- Who is involved in the identification of the unlicensed and unauthorized software (organization/classification);
- How comparisons are performed to identify legal versus unlicensed and unauthorized software;
- How unlicensed and/or unauthorized software is reported;
- Who receives the reports of unlicensed and unauthorized software; and
- How unlicensed and unauthorized software is removed from computers.

3.3 Secure Repository

A secure and protected repository prevents loss, theft and unauthorized use of software, licenses and documentation. To the extent possible, repositories should be kept in a centralized storage area within each facility.

The SMP must address:

- What physical repositories are used (e.g. file cabinet, locked room) and their locations (e.g. centralized, decentralized);
- Who has access to the repositories (organization/classification); and
- What check out procedures are used to remove and return software and documentation to the repositories.

3.4 Ongoing Inventory And Control Methodology

Once the software base is examined in the initial "baseline" inventory, ongoing control processes and procedures must be in place to ensure that the inventory records are updated and remain complete and accurate. New software acquisitions must be added to the inventory and removed software must be deleted. In addition, periodic inventories should be conducted to verify software records and monitor ongoing compliance with the Software Management Policy. For these subsequent inventories, it may not be practical to include all computers. A sample of computers may be inspected.

The SMP must address:

- Who is responsible for developing, implementing and maintaining the ongoing inventory control processes and procedures;
- What ongoing inventory control processes and procedures are used to address receipt and installation of software, removal, and disposal of software and change control;

- Who is responsible for ensuring the inventory control processes and procedures are continuously followed;
- Who conducts the ongoing inventories (organization/classification);
- What processes/procedures are in place to ensure the ongoing inventories occur and who is responsible for them;
- What methodology is used to sample the inventory (e.g. by sub-unit, by geographical location);
- How is the sample size determined; and
- How often will sample inventories occur (e.g. monthly, quarterly, every six months).

3.5 Internal Audits

Effective software management is a continual process and includes audits. The objective of the ongoing audits is to determine the ongoing compliance with software license agreements. These periodic spot checks will identify if unlicensed software has been deliberately or inadvertently installed on an agency's computers. The audit program should also examine the agency's software procurement and record maintenance processes as well as the means by which staff are informed of appropriate software usage.

The SMP must identify:

- Who performs these audits (organization/classification);
- Who is notified of the results of the audit; and
- How results are communicated (e.g. forms, reports, presentations).

3.6 Corrective Actions

Corrective action must be taken when unauthorized use of software is identified. Corrective action is needed 1) when there is a breach of copyright law or the terms of a software license, or 2) when inventory reveals unlicensed copies of software. If either situation is identified, the software programs must be deleted immediately. If ongoing use of the software is needed, immediate action should be taken to correct the licensing breach with the manufacturer.

The SMP must address:

- Who is responsible for corrective actions (organization/classification);
- How corrective actions are accomplished;
- Who is notified of the corrections; and
- How infractions are kept from reoccurring (e.g. education, changes in process, more monitoring, up-dating the list of supported software, re-evaluating the need for additional software licenses).

3.7 Contractors' Certification

The Software Management Policy requires that state contractors certify they have appropriate systems and controls in place to ensure that state funds will not be used in the performance of a contract for the acquisition, operation or maintenance of computer software in violation of copyright laws. These requirements are to be incorporated as standard language in contracts awarded by the state.

The SMP must address:

- Who ensures that certification has occurred (organization/classification);
- How the responsible individual receives certification of compliance (e.g. written statement from contractor, written clause in a contract);
- What controls are in place to ensure appropriate measures are being taken to ensure compliance; and
- What measures are taken if contractors do not comply.

3.8 Disposal Of Hardware And Software

All hardware and software that is no longer to be used in state service shall be disposed of in an appropriate manner. Software should be destroyed to ensure that it cannot be re-used. Hardware can be recycled, except for those components which must have a license. Hard drives should be wiped or scrubbed to remove software as necessary to comply with terms of the software licenses.

The SMP must address:

- Who is responsible for disposal of software and hardware components (organization/classification); and
- The procedures in place to ensure software and hardware are disposed of properly.

4.0 Roles And Responsibilities For The Administration Of The Software Management Program

Roles and responsibilities for the administration of the software management program and the development of the SMP need to be defined within each state agency.

The SMP must identify:

- What are the roles and responsibilities of the department's executive staff?
- What are the roles and responsibilities of department management?
- What are the roles and responsibilities of user's of computer resources?
- What are the roles and responsibilities of the Software Management Team?

5.0 Action Plan

The SMP must include an action plan which lists those activities that are in alignment with SAM Section 4846 – 4846.2. If the department is currently compliant through administration of the Desktop and Mobile Computing Policy or other internal efforts, it can demonstrate that compliance through the submission of current software management documentation. If not currently in full compliance, the department must include an action plan for achieving compliance as part of the Software Management Plan.

Include in the action plan those steps needed to:

- Obtain and maintain a current full software inventory;
- Detect any unlicensed and unauthorized software;
- Provide the secure repository for all software media and licenses;
- Maintain a process for ongoing inventory control;
- Establish and maintain a software management audit program and institute that program as an ongoing effort;
- Establish and maintain the responsibility and processes for taking corrective actions when software breaches are identified;
- Maintain a means to ensure the contractor certifies to appropriate software usage; and
- Maintain a consistent and structured process for disposal of software and hardware.

The action plan should also identify those steps for the preparation of the follow-up software management report to be submitted to the OCIO.

6.0 Timeline

The SMP must include a timeline that identifies when those tasks listed in the action plan discussed above will be completed. If the department can demonstrate compliance with the Executive SAM Sections 4846 – 4846.2 through current documentation, it will not be required to provide a timeline in the SMP.

7.0 Authorized Software List

A current list of authorized software will assist in guiding what software is appropriate and legal for each organization. The list should show all classes and subclasses of software necessary to meet the agencies business needs and, within each class and subclass, which products and product versions will be supported and the category of employees using the product.

The SMP must include a copy of the agency's most current authorized software list.

8.0 Software Management Education

It is essential to have an education effort so that all staff can receive training in the legal use of software and good software management practices. Employee education should

include the individual agency's policies and procedures relating to software management as well as statewide policies. Training should be customized to meet the specific audience needs (users, procurement staff, management, technical staff, and executives). Software management education can be incorporated into normal employee orientation and other training opportunities.

The SMP must address how the state agency will ensure that staff is made aware of software copyright laws and good software management practices.

9.0 Newly Established Agencies and Departments

Newly established agencies and/or departments are required to submit an SMP in conjunction with their Desktop and Mobile Computing Policy.

Newly established state agencies and/or departments will submit to the OCIO a Software Management Report proposing the plan the agency will implement in order to comply with the Software Management Policy. The report shall include:

1. Procedures on how the agency and/or department will:
 - a. Conduct a 100 percent inventory of the agency's software to create a baseline and how that baseline was conducted;
 - b. Detect and remove illegal and unlicensed software;
 - c. Provide for a secure repository of software media, and licenses;
 - d. Provide ongoing inventory tracking and monitoring of new purchases and installations;
 - e. Perform periodic internal audits and ensure appropriate corrective actions are taken when necessary;
 - f. Receive certification from its contractors and bidders that they have appropriate systems and controls in place to ensure that state funds are not used to acquire, operate, or maintain computer software in a manner that does not comply with applicable copyrights;
 - g. Ensure proper disposal of hardware and software consistent with license requirements.
2. A statement of the roles and responsibilities within the agency for the administration of the software management program and enforcement of policy;
3. An action plan detailing the steps to full implementation of the software management policy;
4. A timeline for full implementation of the software management policy;
5. A list of the agency's currently supported software;
6. A plan for employee orientation and education.

10.0 Certification and Compliance

Annually, each agency and/or department will submit to the CIO a certification report declaring they are in compliance with SAM Sections 4846 – 4846.2.

State agencies shall retain within their organization, for three years, the annual certification in the form of a Statement of Compliance (see SIMM Section 80) along with the summary of updated inventories and audits conducted by the agency as part of their ongoing software management practices. The certification, to be submitted to the agency CIO, must include the name of the agency representative responsible for ensuring agency compliance with the Software Management Policy. In support of this certificate, each agency must maintain a detailed inventory report that must be made available to the OCIO and/or the Department of General Services upon request, per SAM Section 4846.2.