Reference Guide on Software Asset Management

Purpose

This document sets out general guidelines on software asset management (SAM) for reference by Government bureaux and departments in implementing their respective SAM measures. Other organisations including the Non-Government Public Organisations may also make reference to this document and make necessary customisation for suiting their own purposes.

2. The guidelines comprise ***basic requirements*** as well as ***good practices***. While an organisation implementing SAM should meet all the ***basic requirements*** stipulated herein, they can choose to adopt some or all of the ***good practices***, with due consideration of factors such as the extent of software use and the availability of resources in their organisation.

3. Please note that the materials provided in this document are not meant to be exclusive nor exhaustive, users of this guide should make reference to other relevant guidelines and Ordinance for implementing their SAM measures.

General

4. Organisations implementing SAM should at least make reference to the Copyright Ordinance details of which can be found on the website of the Intellectual Property Department at: *http://www.ipd.gov.hk/eng/intellectual_property.htm.*

5. It should be noted that, according to the Copyright Ordinance, it may constitute civil and/or criminal offence to possess or distribute an infringing copy for trading or business purpose. Employee who is in possession of pirated software for selling, letting for hire, or for use by others may be liable to criminal prosecution.

6. In particular, the following points regarding liability and copyright infringement should be noted:

- ➢ There may be civil liability, both on the part of the Government employee concerned and on the part of the Government, where the Government employee possesses or distributes pirated software in the course of his employment.

- ➢ The copying, renting copies and making adaptation of software without licence of the copyright owner are all infringing acts.

- ➢ It is a criminal offence for a person to, without the licence of the copyright owner, possess an infringing copy of the work with a view to its being sold or let for hire for the purpose of or in the course of any trade or business.

Definition

7. For alignment of understanding, definitions of some specific terms used in the context of this guide are provided below:

- ➢ "***unauthorized software"*** means software which is not licensed for use, or software the use of which has not been authorized by the head of an organisation.

- ➢ ***"Intellectual Property Compliance Officer (IPCO)"*** is an officer who is appointed to oversee matters related to SAM and intellectual property protection. An officer of the appropriate rank should be appointed as the IPCO to monitor SAM related activities at all levels of the organisation. Sufficient training on SAM and intellectual property protection should be arranged for the IPCO.

Basic Requirements

8. **Some** Basic Requirements for the implementation of SAM are listed below, with some suggested actions for implementation provided along-side:

Basic requirements	***Suggested actions***
Promulgate internal instructions to enforce the proper management and use of computer software	● Internal instructions should be promulgated: ➢ to require staff to follow organisational guidelines on the proper use of software (see **Annex A** for a suggested list of points to note); ➢ to stipulate that staff who breach such guidelines would be liable to disciplinary actions; and ➢ to highlight the different level of disciplinary actions that may be instigated, with more severe sanctions against the use of pirated software.

Ensure general awareness of all staff to use only authorized software	● Regularly (say, every 3 months) promote the general awareness of using only authorized software in the organisation. For instance, remind staff regularly by re-circulating the relevant circulars and guidelines, and ask them to sign to acknowledge having read and understood the requirements of the circulars and guidelines. ● Make known to all staff the management structure, policies and procedures pertinent to SAM. ● Develop simple questions and answers on SAM for reference by all staff.
Establish procedures for acquiring software legitimately	● Clearly define, document and enforce the acquisition procedures, which should be readily accessible to all staff. ● Standardise and centralise the acquisition of all software through a central office. The staff in this office should be well-trained in general licensing requirements and be wary of possible risks of infringing intellectual property rights of software. (See **Annex B** for types of unauthorized software and **Annex C** for signs of illegally copied software.) ● Demand and verify proper licences and accompanying materials from suppliers when software is acquired, including pre-loaded software, downloaded freeware and shareware. ● Consider software and hardware as separate line of items for budgeting and procurement purposes so as to avoid purchasing computers with unauthorized software pre-loaded onto them. This also prevents users from using unauthorized software because of insufficient funds for procuring software. ● Disallow reimbursement of any user expense that is expended for software acquisition.
Keep all software licences	● Retain all relevant certificates and documents, including licences, media, completed registration cards, invoices and documentation in a central and secure location.
Maintain an up-to-date software inventory of all	● Undertake an initial inventory of all supported software to include the following information:-

software used	➢ identification number of the computer on which the software is installed ➢ location of the computer ➢ product description of the software ➢ licence number of the software ➢ effective licence period ➢ other licence information such as whether it is an upgrade of licence or it is an Original Equipment Manufacturer (OEM) licence ➢ date of purchase of the software ● Define and document the procedures for maintaining the software inventory. ● Regularly take inventory of software purchased, being used and disposed of, say every 3 to 6 months, in order to maintain an up-to-date inventory.
Confirm the legality of all software used regularly	● Institute apparatus, like software audits, of checking whether all software installed is authorized. ● Enforce stringent software installation procedures, for e.g., installing software on computers by a central office before allotting computers to staff.

Good Practices

8. Some Good Practices for the implementation of SAM are listed below, with some suggested actions for implementation provided along-side:

Good practices	*Suggested Actions*
Appoint an Intellectual Property Compliance Officer (IPCO) to oversee matters related to SAM and intellectual property protection	● An officer of the appropriate rank should be appointed as the IPCO to monitor SAM related activities at all levels of the organisation. ● Sufficient training on SAM and intellectual property protection should be arranged for the IPCO.

Define procedures for installing and distributing software	● Clearly define and enforce procedures for software distribution and installation, ensuring all software installed is authorized. In particular, the requirement of prior authorization for installing software on computer has to be clearly defined. ● Clearly define responsibilities for software distribution and installation. ● Update the inventory after installing the software.
Conduct software audits regularly	● Compile a list of software installed in computers, including servers. ● Reconcile the number of installed software against the total number of licences permitted so as to ensure that there is no overuse of licence. ● Match the list against the software inventory to ensure software installed is authorized. ● Undertake follow-up actions, such as: ➢ When an upgrade to a piece of software is purchased, you may be required to dispose the old version, depending upon the purchase agreement; ➢ When any unauthorized software is identified, all staff should cease using the software immediately. The matter should be reported immediately to the Intellectual Property Compliance Officer of your organisation for investigation and further actions; ➢ Organisation should review the need to acquire the necessary licences for the software; ➢ For any suspicion of committing a criminal offence as set out under Section 118 of the Copyright Ordinance (Cap. 528), organisation should report the matter to the Customs and Excise Department for criminal investigation; ➢ Update the software inventory in case of any discrepancies. ● Conduct survey on the software needs of staff and review the list of supported software. This would help ensure that staffs have what they need in carrying out their works and there is adequate licence coverage.

Use automated SAM tools in managing software assets	● Select SAM tools with software inventory and metering functions. Software inventory scanning tools can help detect unauthorized software installed, while software metering tools can help prevent the use of software which has exceeded the number of licences purchased for the software in a networked environment.

Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region
July 2008

Annex A

Points to note on the proper use of software

- Do not use unauthorized software in your computer. When an upgrade to a piece of software is purchased, you may be required to dispose the old version, depending upon the purchase agreement. When any unauthorized software is identified, all staff should cease using the software immediately. Such case should be reported immediately to the Intellectual Property Compliance Officer for investigation and further actions. Organisation should review the need to acquire the necessary licences for the software. For any suspicion of committing a criminal offence as set out under the Copyright Ordinance (Cap. 528), organisation should report the matter to the Customs and Excise Department for criminal investigation.

- For group-licensed software, ensure that software copies installed do not outnumber software copies purchased.

- When upgrades of software are purchased, the old version may be required to be disposed of depending on the purchase agreement.

- If the software is pre-loaded in a new computer, check whether the software comes with a proper licence and get the relevant certificates.

- Do not copy or modify software without the express permission of the copyright owners save where the statutory exceptions apply. (*Under the Copyright Ordinance, a lawful user of a copy of a computer program may make a back-up copy of the program, without infringing the copyright in the program, if it is necessary to have the back-up copy for the purposes of his/her lawful use. Furthermore, a lawful user of a copy of a computer program may copy or adapt the program without infringing the copyright in the program if the copying or adapting is necessary for his/her lawful use, e.g for the purpose of correcting errors in it.*)

- Software owner should remove the software on loan to others from his/her computer first before delivering to the borrower. The borrower should remove the software from the computer after use, before returning the software to the owner.

- For software licensed for organisation use, staff should not copy it for their personal use.

- To impose a tighter control on the use of software, staff should not:-
    - bring software licensed personally to office to carry out office work without permission of the head of the organisation;
    - install or use unauthorized software, including those software that do not require installation (e.g. portable software stored in removable storage devices); and
    - download software from the Internet without the permission of the head of the organisation. Even if proper permission has been obtained from the head of the organisation, one has to ensure that the licence agreement set out by the copyright owner is strictly adhered to before using the software.

Annex B

Types of unauthorized software

Staff responsible for evaluating bids or engaging in negotiations to acquire computer software should be cognizant of the different types of unauthorized software. Unauthorized software includes both illegal software and legitimate software (licensed but misused software) that violates licensing restrictions.

Types of illegal software	
Counterfeit software	Unauthorized copies of software that are duplicated with the intent of directly imitating the copyrighted product. Counterfeit software is typically reproduced and distributed in a form to make the product appear legitimate and thus may include sophisticated efforts to replicate packaging, documentation, registration logos, and security features.
Compilation CDs	Unauthorized copies of multiple software programs that are compiled onto a single CD. Compilation CDs typically include software programs published by a variety of manufacturers.
Hard disk loaded software	Unauthorized copies of software loaded by the hardware dealer onto the hard disk of the computer and then offered to the customer for free or with a big discount for sale promotion.
Online	Unauthorized copies of software that are downloaded via a modem to an electronic bulletin board or the Internet.
Other illegally copied software	Software that is copied from disks, CDs or other machines, without the authorisation of the copyright owner.

Types of licensed but misused software	
Original Equipment Manufacturer (OEM) software	OEM software is licensed and specifically marked for distribution with new computer hardware. Licence misuse occurs when OEM software is unbundled from the computer and distributed to, and used by, the end user as a standalone product.
Academic versions	Academic software is manufactured, licensed and specifically marked for distribution to educational

	institutions and students at reduced prices. Licence misuse occurs when academic software is distributed to, and used by, a non-academic end user.
"Not For Resale" software	Software marked "not for resale" is typically distributed as promotional or sample product and not licensed for commercial distribution and use. Licence misuse occurs when such software is distributed in violation of its resale restrictions.
Fulfillment software	Fulfillment software is licensed solely for distribution to mid- or large-sized end users that currently possess a volume licence agreement or valid site licence. Fulfillment software is typically distributed in a CD jewel case without the packaging or materials that accompany retail product. The fulfillment media is not itself licensed product. Licence misuse occurs when fulfillment software is distributed to, and used by, end users that lack the necessary licences for use of the underlying product.
Software upgrades	Upgrade versions of software programs that are licensed and specifically marked for distribution to end users that currently possess a valid licence for the original product. Licence misuse occurs when upgrades are distributed to, and used by, end users that lack a licence for the original product.

Annex C

Signs of illegally copied software

- The price of the software is significantly lower than the manufacturer's suggested retail price or otherwise appears "too good to be true".

- The software is distributed in a CD jewel case without the packaging and materials that typically accompany a legitimate product.

- The software lacks the manufacturer's standard security features, such as a hardware lock or certificate of authenticity.

- The software lacks an original licence or other materials that typically accompany legitimate products (e.g. original registration card or manual).

- The packaging or materials that accompany the software have been copied or are of inferior print quality.

- The CD contains software from more than one manufacturer, or programs that are not typically sold as a suite.

- The software is downloaded via the Internet without the manufacturer's authorisation.

- The software is distributed via a mail order or online reseller that fails to provide appropriate guarantees of legitimate product.

- The software contains markings indicating that distribution to, and use by, the organisation would violate the manufacturer's licence (e.g. distribute only with new PC hardware, academic version, upgrade, etc.).

- The software is loaded onto computer hardware without a separate licence or invoice indicating a legitimate purchase.