Governments all over the world are increasingly viewing information and communication technology (ICT) as a critical element which empowers states to better use their national resources and improve public services delivery. The international call for governments to respond to standards of accountability, transparency and participatory governance has highlighted considering ICT as an essential ingredient of ‘good governance’ and as an engine for sustainable development and growth.

Within this context, the Office of the Minister of State for Administrative Reform (OMSAR) in charge of, since its inception in 1994, to develop plans and design
solutions based on the latest developments in information and communication technology and its implementation for the State benefit, is presenting this practical guide as a reference tool for Software Asset Management (SAM) in the Public Sector. A select number of key ICT policies and procedures for SAM and the appropriate good practices relevant to the fulfillment of these processes are presented in this guide along with pertinent reference materials.

The Guide is intended for the use by ICT units and concerned staff in the government, yet its broad contents make it suitable for all ICT or technical personnel regardless of their employer. As such, the Guide can be viewed as another initiative meant to develop ICT on the National level and in various sectors.


العام. يحتوي الدليل على عدد من السياسات الأساسية لتكنولوجيا المعلومات والاتصالات والإجراءات اللازمة لأصول إدارة البرمجيات إضافة إلى الممارسات السليمة المناسبة المتعلقة بإنجاز هذه العمليات، وقد تم توثيقها بشكل ملحقات للدليل.

وعلى الرغم من أن هذا الدليل مخصص للاستعمال من قبل وحدات تكنولوجيا المعلومات والاتصالات والموظفين المعينين في الإدارة العامة، إلا أن مضمونه الشامل يتيح الاستفادة منه لكافة اختصاصيي المعلومات في جميع المجالات. كذلك يمكن اعتبار الدليل مرجعاً عاماً لتطوير مبادرات تكنولوجيا المعلومات والاتصالات على المستوى الوطني وفي مختلف القطاعات.

ولتسهيل عملية استخدام الدليل قام مكتبنا بإصدار نسخ رقمية كاملة على أقران مدفعة تفاعلية، ونشر محتوياته على موقع مكتب وزير الدولة لشؤون التنمية الإدارية على شبكة الإنترنت (www.OMSAR.gov.lb) بحيث يمكن وصول الموقع ونقل مقاطع محددة من الدليل بشكل فردي، بالإضافة إلى إن هذه القنوات الرقمية تتيح الوصول إلى الدليل والتحديث الفوري لمحتوياته.
where updates to the various sections of the Guide can be accessed and downloaded.

The production of this Guide by OMSAR further highlights its leading role in supporting and introducing latest ICT development and modern institutional reform intending to constantly provide the Lebanese Public Administration with the facilities and tools needed to ensure that investment in ICT resources achieves the required returns on one hand and to keep track with International ICT developments and best practices on the other hand.

Mohamad Fniesh
Minister of State for Administrative Reform
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Requirement Definition Policy</td>
<td>a) Introduction</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>i. Overview</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>b) Requirements Specification</td>
<td>15</td>
</tr>
<tr>
<td>2. Software Acquistion Policy</td>
<td>a) Introduction</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>i. Overview</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>b) Software Acquisition Steps</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>i. Requesting Software</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>ii. Purchasing Software</td>
<td>17</td>
</tr>
<tr>
<td>3. Receiving Software Policy</td>
<td>a) Introduction</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>i. Overview</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>b) Receiving Software</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>i. Distributing Software</td>
<td>23</td>
</tr>
</tbody>
</table>
ii. Software Documentation

4. Software Installation Policy

a) Introduction
i. Overview

b) Policy
i. Software Installation
ii. Risks of unauthorized software installations
a) Software licensing
b) Increased support costs
c) Malicious software
d) Other vulnerabilities

iii. Auditing

5. Software Use Policy

a) Introduction
i. Overview

b) General Policies
i. Software from other sources
ii. Additional copies
iii. Unauthorized copies
iv. Internal controls
6- Software Maintenance Policy
   a) Introduction
      i. Overview
   b) Policy

7- Software Disaster Recovery
   a) Introduction
      i. Overview
   b) Inventory
   c) Installation Media
   d) Proof of Ownership

8- Retiring Software Policy
   a) Introduction
      i. Overview
   b) Retiring Software
The Lebanese Government has undertaken a series of initiatives over the past years to develop policies that make use of ICT to promote transparency, reduce its operations cost and increase the effectiveness of its service delivery.

The Office of the Minister of State for Administrative Reform (OMSAR), being the lead government entity in promoting the adoption of ICT as a tool for administrative development, was aiming at a process through which the Lebanese administration collects, organizes, accesses, analyzes, and shares information on a scale and with unprecedented efficiency.

Within this framework, OMSAR, in association with Microsoft, launched SAM (Software Asset Management) as a multi-phased project that aims to lay down the framework of the Lebanese administration to manage its software assets and improve its administrative efficiency.
foundation in which the Lebanese Public Administration should address their software requirements. This project also assists in building the capacity of IT managers by making them aware about SAM and its applications in order to attain lower cost with higher efficiency, transparency and accountability. The production and dissemination of this Guide is considered to be a basic task in this project.

This ambitious project strives for eliminating the methods utilized in the early days of acquiring and using software applications and for replacing them with a scientific and systematic approach derived from international standards and best practices.

This new approach introduces an effective management plan to address asset acquisition, use and disposal. It considers that ICT, with its hardware and software components, must be managed throughout their lifecycle like other valuable assets in order to achieve its potential benefit. More importantly, by knowing precisely what
software assets exist on the network, decisions based on solid information can be made with regard to all future software procurement which additionally places the administration in an excellent position when negotiating future ICT purchases.

This Guide is intended to be used by various ICT units within the Public Sector and by other technical personnel who will benefit from the procedures and guidelines therein.

In its initial phase, the project aims at distributing this Guide in a printed format with a CD-ROM attached. Also, the content of this Guide will be placed on OMSAR’s website (www.omsar.gov.lb).

OMSAR will be committed to follow up on the usage of the Guide by the departments in the Public Sector and shall use all feedback and commentary to enhance and update the initial material produced in it.
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)’s internal procedures.

This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

This is the phase during which the requirements for a new application are gathered, based on the business needs of the organization. It covers business functional and technical requirements to enable (Entity Name) to minimize the cost to acquire and implement the right solutions whilst ensuring that they enable the organization to achieve its business objectives.
i. Overview

Requirements specification ensures the delivery of an operable and manageable system which provides the required functionality under all situations.

b) Requirements Specification

When selecting a software package those detailed requirements are a valuable input for the RFP (Request for Proposal).

- System Availability
- Support Hours
- Performance Requirements
- Troubleshooting
- Recoverability and Data Integrity
- Reliability
- Manageability
- Backup and Recovery
- Performance
- Scalability
- Installation Requirements
- Configuration Requirements
- Maintainability Requirements
- Localization / Internationalization Requirements
- Documentation Requirements
- Monitoring

ب) مواصفات المتطلبات

عند اختيار مجموعة من البرامج تشكل هذه المتطلبات التفصيلية مساهمة قيمة لطلب تقديم العروض.

- توفر النظام
- ساعات الدعم
- متطلبات الأداء
- حل المشاكل
- إسترداد وتكامل البيانات
- الفعالية
- السهولة في الإدارة
- النسخ الاحتياطيّة وإسترداد البيانات
- الأداء
- التدريب
- متطلبات التثبيت
- متطلبات التعديل
- متطلبات الصيانة
- الأقلمة/متطلبات التدويل
- متطلبات التوثيق
- المراقبة
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)'s internal procedures.

This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

i. Overview

(Entity Name) recognizes the importance of the legal and ethical use of software licenses by ensuring that all software packages (Entity Name) purchases are legal and appropriately accounted for.
b) Software Acquisition Steps

1. Requesting Software

Determine your software business requirements and work with the IT department to translate business requirements into a high-level design specification for software acquisition (see Requirements Definitions Policy).

Obtain the approval of the requesting department manager and IT manager on the gathered requirements.

2. Purchasing Software

In case of proprietary software,

The policy guidelines for acquiring new application software are as under:

- If the required software price doesn’t exceed purchasing price threshold (Amount) (e.g. 5 million LBP), the requesting department sends the completed purchase order (PO) requisition to the IT Department for verification and approval. If changes are necessary, IT
The IT Department sends the approved purchase order requisition to the Purchasing Department where it is processed.

If software price exceeds the purchasing price threshold (Amount), the Procurement Department must prepare a Request for Proposal (RFP); otherwise IT department selects a vendor and executes the purchase order.

The RFP is advertised.

The Procurement Department will receive all the responses to RFP for a close scrutiny.

After examining the RFP response, the Procurement Department must short-list (number) vendors whose product is considered to be close to meeting most of the business requirements.

If possible the vendors should be asked to arrange on-site visits to demonstrate the use of their products.
These on-site visits should focus to get information on the following points:

- Reliability: Is the product reliable?
- Commitment to Service: Is the vendor responsive to problems with the product? Can he deliver on time?
- Customization: Has the vendor customized the product in time and within the estimated cost?
- Financial Standing: Has the vendor good reputation and financial strength?
- Training & Support: What is the level of user satisfaction on training and support given by the vendor?

Based on the response of RFP & the site visits, the Head of Procurement Department and the Head of IT Department decide on the final selection of a vendor.

The last step in the software acquisition process is to negotiate and sign a formal service level agreement.
(SLA) with the vendor. This must be done by the Procurement Department before releasing any payment to the selected vendor.

When considering open source alternatives, first consult with the IT Department regarding the rights and responsibilities conferred by the particular open source license or code-sharing agreement associated with the solution. IT Department then proceeds to acquire the open source software.

Software provided as grant or purchased by another party must be escorted by all significant licensing information and delivered to the Purchasing department for processing.

Procurement Department maintains and manages all contracts, licenses and proof of entitlements. IT department must have access to all licensing information in order to maintain software inventory, review entitlements and verify with software procurement. This must be done by the Procurement Department before releasing any payment to the selected vendor.

When considering open source alternatives, first consult with the IT Department regarding the rights and responsibilities conferred by the particular open source license or code-sharing agreement associated with the solution. IT Department then proceeds to acquire the open source software.

Software provided as grant or purchased by another party must be escorted by all significant licensing information and delivered to the Purchasing department for processing.

Procurement Department maintains and manages all contracts, licenses and proof of entitlements. IT department must have access to all licensing information in order to maintain software inventory, review entitlements and verify with software procurement. This must be done by the Procurement Department before releasing any payment to the selected vendor.
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)’s internal procedures.

This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

i. Overview

The purpose of this document is to outline the steps we need to take in order to ensure that all purchased software is properly received and its information is processed into our inventory tracking system and all documentation of ownership is properly stored and maintained.
b) Receiving Software

When the item(s) is/are received, the IT Department follows (Entity Name) Check-In Procedure to ensure the software is included in the software inventory. (see software check-in checklist.pdf)

IT department enters the software into the inventory database including the following details:

• Software Description
• Software Type
• Software Serial Number
• Date of purchase
• Date of delivery
• Supplier
• Proof of license reference
• License Types
• Number of licenses entitled.

Receipt of software must be verified on the purchase order by the assigned personnel or committee.

The purchase order is sent to the accounting department escorted with the invoice to process payment.
Software purchased and downloaded from the internet must be burnt on CD/DVD and escorted with their licensing information, serial numbers, and any other significant material to be stored at the remote storage location.

The IT Department maintains such copies of media and documentation as needed to support our systems in a central on-site repository. All remaining original and backup disks and all original licensing documentation, keys, and manuals are stored offsite in a fire/water proof safe at the following location:

• (Address 1)
• (Address 2)

i. Distributing Software

After the check-in process is complete, IT Department will contact the requesting department to schedule software installation.

IT will require the following information for each employee who will receive the software:

1. توزيع البرامج

بعد اكتمال عملية فحص البرامج يقوم قسم تكنولوجيا المعلومات بالاتصال بالقسم المعني بالطلب لجدولة تثبيت البرامج.
• Name
• Email Address
• Phone Extension

If software needs to be reinstalled, contact IT Department to perform the reinstallation.

ii. Software Documentation

Copies of the End User License Agreement (EULA) and manuals will be made available to the department(s) receiving the software.

If, at any time, an employee needs a copy of software documentation, the IT Department will provide the documentation.
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)’s internal procedures.

This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

i. Overview

This policy applies to all of the organization’s machines, and sets the required procedures to install additional software to (ENTITY NAME) machines.

أ) المقدّمة

هذه سياسة عامة ويجب تعديلها من أجل تلبية الإجراءات الداخلية ل (إسم الإدارة).

هذه السياسة لا تتعلق ببائع برامج محدد بل تنطبق على جميع أنواع البرامج (برامج المنهجية، برامج الأنظمة، برامج التطبيق، برامج إدارة المخزون، برامج الاستخدام، برامج الحفظ الاحتياطي واسترداد البيانات، الخ...)

1. لمحة عامة

تتطبق هذه السياسة على كل أجهزة الشركة، وتحدّد الإجراءات المطلوبة لثبيت برامج إضافية لآلات (إسم الإدارة).
b) Policy

i. Software Installation

Authorized software installation should be performed as a centralized process through the IT Department. No additional software may be installed on any machine without the approval of the IT Department. Installation of unauthorized software could result in either making the computer system unstable, unsecured or subjecting the organization to additional licensing liabilities.

Software Installation Request Process:

1. Requester has to fill out the following Software Installation Request Form and submits it to IT Department.
2. The form has to be approved by the Department Manager in order to be acted on.
3. In case of new software, it has to first be tested and validated for installation on (ENTITY NAME) computer systems.
4. IT Manager approves the Installation Request Form.

5. Software asset inventory is checked for license entitlement.

6. Software installation is completed in the same order as received.

7. If existing, software manual and or training material is delivered to the requesting department.

8. Software asset inventory is updated.

ii. Risks of unauthorized software installations

a) Software licensing

One of the primary reasons why it is important to prevent unauthorized software installations on workstations is because of tricky software licensing issues.

b) Increased support costs

Users are also not allowed to install applications of their own as this will result in great increases in support costs.
c) Malicious software

Another reason for not allowing software installation is because of the threat of malicious software. There are two different types of threats that should be considered when it comes to malicious software. One is malicious software that is piggybacked onto legitimate software. The Internet is chock-full of freeware applications that are bundled with adware or spyware modules.

The other type of malicious software is the type that gets installed without the user's knowledge or consent.

d) Other vulnerabilities

One last reason why a good software installation policy is important is because unauthorized software can increase the chances of the system being exploited. There is a standard of computing that states that the greater the amount of code that's
executing on the system, the better the chances that the code will contain at least one critical security vulnerability.

iii. Auditing

The IT Department has the right to audit all (ENTITY NAME) machines for unauthorized software installation. The IT Department will on random basis select a set of computers to check for unauthorized software installed into the machines. The audit is done on random dates and random machines. In case unauthorized software was found, the software will be automatically uninstalled and the user will be warned of repeating the action. Results of the audit will be documented and kept for each audited machine.
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)’s internal procedures.

This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

i. Overview

(Entry Name) recognizes the importance of the legal and ethical use of software assets. This document provides guidelines for employees to follow to ensure that we are both legal and ethical in the use of our software assets. All software assets
are for business use only and should not be used by employees for personal interests.

b) General Policies

(Entity Name) has acquired fully licensed copies of computer software from a variety of publishers and vendors. Licensed and registered copies of software programs are placed on computers within (the Entity) and appropriate backup copies made in accordance with the licensing agreements and (Entity) policies. No other copies of this software or its documentation can be made without the express written consent of the software publisher and (Entity Name).

i. Software from Other Sources

(Entity Name) will provide copies of legally acquired software to meet all legitimate needs in a timely fashion and in sufficient quantities for all of our computers. The use of software obtained from any other source is for business use only and should not be used by employees for personal interests.
(e.g. downloaded software, pirated software, cracked software, etc...) could present security and legal threats to the (Entity), and such use is strictly prohibited.

ii. Additional Copies

In some cases, the license agreement for a particular software program may permit an additional copy to be placed on a portable computer or home computer provided only one user uses both installations. Employees will not make such additional copies of software or documentation for the software without the approval of (Entity Name) IT Department. When legal, approval will be granted for such installations when there are valid business reasons.

iii. Unauthorized Copies

The unauthorized duplication of copyrighted software or documentation is a violation of the law (Law on the Protection of Literary and Artistic Property No. 75 of April 3, 1999) and the management, and the software trademarked, etc...) can represent security and legal threats to the (Entity), and such use is strictly prohibited.

2. Additional Copies

In some cases, the license agreement for a particular software program may permit an additional copy to be placed on a portable computer or home computer provided only one user uses both installations. Employees will not make such additional copies of software or documentation for the software without the approval of (Entity Name) IT Department. When legal, approval will be granted for such installations when there are valid business reasons.

3. Unauthorized Copies

The unauthorized duplication of copyrighted software or documentation is a violation of the law (Law on the Protection of Literary and Artistic Property No. 75 of April 3, 1999) and the management, and the software trademarked, etc...) can represent security and legal threats to the (Entity), and such use is strictly prohibited.
(Entity Name)’s policy. Employees should not make, acquire or use unauthorized copies of computer software or documentation.

iv. Internal Controls

(Entity Name) reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorized copies of software. These controls may include periodic assessments of software use, announced and unannounced audits of (Entity) computers to assure compliance, the removal of any software found on (Entity Name) property for which a valid license or proof of license cannot be determined.
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)’s internal procedures.

This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

i. Overview

The purpose of this policy is to ensure computer systems attached to the (ENTITY NAME) network are updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits. These mechanisms are intended to
reduce or eliminate the vulnerabilities and exploits with limited impact to the business.

This policy applies to all (ENTITY NAME) employees. Any other parties, who use, work on, or provide services involving (ENTITY NAME) computers, technology systems, and/or data will also be subject to the provisions of this policy.

b) Policy

1. All networked devices will be patched with vendor provided operating system security patches.

2. These patches will be downloaded to a central server and then deployed to all other machines as soon as the appropriate testing is completed by (ENTITY NAME) IT Department.

   • IT Department must first apply new patches on an isolated testing environment to make sure that they don’t cause malfunction or system breakdown.

   • After passing the testing process,
patches get approved by the IT Manager for direct deployment.

3. New devices must be patched to the current patch level, as defined by the operating system vendor, PRIOR to the device being connected to the production network.

4. (Windows System Update Services (WSUS) or System Center and Configuration Manager (SCCM)) is used for downloading, installing and distributing windows updates automatically.

5. (Tool Name) (e.g ManageSoft, Opatch, Microsoft SCCM with Quest Extensions) is used to install (non-Microsoft products’) patches and updates into servers and client computers.

6. Log for patches must be maintained on the central server for tracking and monthly security review checks.

• بعد إجتياز عملية الاختبار، تتم الموافقة على التّصحيحات من قبل مدير قسم تكنولوجيا المعلومات لنشرها مباشرة.

3. يجب تحديث الأجهزة الحديثة بالتّصحيحات الحالية كما سيعترف بها بائع نظام التشغيل، وذلك قبل وصل الجهاز بشبكة الإنتاج.

4. يتمّ استخدام نظام Windows لخدمات التحديث (WSUS) أو مركز النظام ومدير التّعديل (SCCM) لتثبيت تحديثات Windows تلقائيّاً.

5. يتمّ إستخدام (إسم الأداة) (مثلاَ: ManageSoft، Opatch مع ملحقات Microsoft SCCM، Quest للثّبت تّصحيحات (غير منتجات مايكروسوفت) لحوادث وأجهزة كمبيوتر الزّبون.

6. يجب متابعة وصيانة سجلّ التّدّهيات والتّصحيحات على الخادم المركزيّ للتعقب والمراجعة الشهريّة للكشف الأمني.
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)’s internal procedures. This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

i. Overview

(Entity Name) recognizes that software is a major tool for all of our lines of business. As such, certain steps need to be taken to protect our investment and ensure maximum continuity of function in the event of a disaster. This plan provides an overview of the steps...
necessary to protect this important part of our business.

b) Inventory

The first thing we have to know is what software we have licenses for. To achieve this goal we will need to maintain a central inventory of all software licensed by the organization. In order to ensure that inventory data is maintained and kept up to date, we will enter all new software into the system upon arrival. We also will conduct regular audits of the system to verify continuing data integrity. Lastly, we will ensure that a full copy of our inventory data is maintained offsite and updated regularly.

The entry of new software into the system will occur as part of a standard software check-in process. This check-in process will be performed before newly arrived software is disseminated for use. This will allow us to ensure that no software is installed without first being entered

بن) لائحة الموجودات

إن أوّل ما يجب معرفته هو ما لدينا من البرامج التي نملك تراخيصها. لتحقيق هذا الهدف، يجب المحافظة على لائحة موجودات مركزية لجميع البرامج المرخصة من قبل الإدارة. ولضمان تحديث بيانات اللائحة والمحافظة عليها، سندخل جميع البرامج الجديدة في النظام فور وصولها. كما سنقوم بمراجعات منتظمة للنظام للتحقق من تكامل البيانات وصلاحيتها. وأخيرا، علينا ضمان نسخة كاملة من البيانات و الحفاظ عليها خارج نطاق الموقع وتحديثها بانتظام.

تشكّل عملية إدخال البرامج الجديدة إلى النظام جزءاً من عملية التحقق من البرامج المُعتمدة لتسجيل إدخال البرامج. ستُنفّذ عملية التحقق من البرامج قبل توزيع البرامج الجديدة للاستخدام. وسيضمن لنا ذلك أنه لن يتمّ تثبيت أيّ من البرامج قبل إدراجه على نظام لائحة الموجودات كما أنّه سوف يفسح المجال لحماية وسائطك ملكيّة الوثائق ووسائل تثبيت البرامج كما هي مذكورة في باقي المستندات.
into the inventory system. This will also provide an opportunity to protect proof of ownership, documentation and installation media as outlined elsewhere in this document.

Regular audits are keys to maintaining the integrity and relevance of our inventory data. We will perform quarterly spot checks to verify inventory counts on a randomly selected cross section of our software and use the resulting counts to update our inventory. On an annual basis we will conduct a full inventory and compare the results to our existing inventory data, spot-checking for any inconsistencies.

We need to maintain an offsite copy of this data to protect ourselves in the event of a disaster that destroys our on site records. This data should be updated on a regular basis to ensure consistency. At a minimum, the offsite copy should be updated whenever an inventory audit is completed. This copy should be housed at a safe location that several people can access in an emergency.
at the organization can gain access to. This will prevent dependence on any one person for access in the event of an emergency.

c) Installation Media

Software installation media also needs to be protected in the event of a disaster, though it should be easily accessible to support staff as well. To ensure safety in the event of a disaster, we will locate copies of all installation media in a protected, offsite location. To provide support staff with needed access we will also keep a central library of installation media available for use. The offsite repository should be updated as regularly as possible.

One original of the installation media for each software title should be set aside and taken to the offsite repository. This media (CD, user manuals, software upgrades, etc...) should always be an original so that it can provide additional proof of ownership if needed. In addition, all
software upgrades and security patches that are automatically downloaded to the central management server are to be regularly backed up and sent for offsite storage. The offsite repository should be updated as often as is feasible, quarterly at a minimum. No more than one copy of media for each version of each software title should be stored offsite in order to minimize the size of the repository.

If the manufacturer permits making backup copies, at least one copy of the software installation media should be filed in the central installation media library for use by our technicians. If copies are not allowed, additional original media will be needed. If we do not own several copies of the software package, and hence several copies of the media, additional copies of the installation media can usually be obtained from the manufacturer for a small fee. Any additional copies of the media should also be stored in the onsite library, to give as much flexibility to our support staff as possible.

 إذا كانت الشركة المصنّعة تصرّح بنسخ احتياطية، يجب على الأقل إبداع نسخة واحدة من وسائط التشغيل في قاعدة البيانات المركزية للاستخدام من قبل الفنيين لدينا. في حال حظر النسخ الإضافية، سيلزم وسائط إضافية أصلية. في حال غياب عدّة نسخ من حزمة البرامج، وبالتالي عدّة نسخ من الوسائط، يمكن الحصول على وسائط التنزيل من المصدر مقابل رسم زهيد. يجب أن تخزن أي نسخ إضافية من الوسائط في المكتبة المركزية في موقع الإدارة، لإعطاء قدر المستطاع من المرونة لموظفينا الدعم التقنيين.

(1) البرهان الملكية

تعتبر وثائق إثبات الملكيّة من أهمّ العوامل في حماية استثمار الإدارة في الأصول البرمجيّة.
d) Proof of Ownership

Proof of ownership documentation is the most important factor in protecting the organization’s investment in software assets. As such, we will send the originals of all such documentation to our offsite repository. We will retain copies of this documentation in an onsite location to assist in the event of a software-license audit.

During the software check-in process we will remove and retain all documentation that pertains to ownership of the software package. This documentation can consist of any or all of the following:

- End User License Agreements
- Certificates of Authenticity
- Purchase Invoices
- Bills of shipment
- Software Boxes (including CD keys, manuals, etc...)

In case of electronic evidences, documents have to be saved in a

على هذا النحو، سوف نرسل جميع النسخ الأصلية من تلك الوثائق إلى موقع 우리 الرفاهي. كما سنحتفظ بنسخ من هذه الوثائق في موقع العمل لتقديم المساعدة في حال حصول تدقيق لرخص البرامج.

خلال عمليّات التّحقق من البرامج سنقوم بإزالة جميع الوثائق التي تتعلّق بملكيّة حزمة البرامج ووضعها جانباً. يمكن لهذه الوثائق أن تتكوّن من أي أو كل ما يلي:

- إتفاقيات ترخيص المستخدم
- شهادات توثيق البرامج
- فواتير الشّراء
- فواتير الشحن
- برمجيات (بما فيه الاحتراز المدمّجة، دلائل الإستخدام، إلخ...)

في حالات الإثباتات الإلكترونيّة، يجب حفظ المستندات في ملفّ آمن محظور الدّخول إليه بإستثناء المستخدمين المخوّل لهم. كما يجب طباعتها وحفظها مع باقي براهين الملكيّة.
secure folder with restricted access to only authorized users. And must be printed and kept with other proofs of ownership.

All of this type of documentation should be retained. The software boxes should be flattened to facilitate storage and all originals should be placed in an envelope and labeled for offsite storage. As always, the offsite storage should be updated regularly to ensure the continuity of our protection.

Whenever possible, photocopies should be made of the documentation and the copies should be kept onsite in a central set of files. This onsite set of copies will provide the proof of ownership needed in the event of an audit, while still allowing us to protect our software assets if disaster strikes.
a) Introduction

This is a general policy and it must be modified in order to meet (Entity Name)’s internal procedures.

This policy is not software vendor specific and it applies to all types of software (programming software, system software, application software, inventory management software, utility software, data backup and recovery software, etc...)

i. Overview

Knowing when to retire your software is just as important as knowing when to purchase it in the first place. Just as it’s important to know exactly what you need, what updates are available and if you really need them, it’s equally important to know when it’s time to
get rid of the old and bring on the new. The money you save can be reinvested in either purchasing new applications or developing your own.

This policy provides guidelines for retiring software and it applies to any software that is a property of (Entity Name).

b) Retiring software

When considering changing your old software. Consider the following:

• Retire software that’s old, under-used or over-maintained.

• Buy only the software that’s really necessary.

• Look for real-time results
  If your old software isn’t giving you up-to-date, up-to-the-minute data and results, it may be time to look elsewhere.

• Return on investment (ROI)
  Invest the organization’s money in

ب) الاستغناء عن البرامج

عندما تقرر الإستغناء عن برامجك القديمة يجب الأخذ بعين الاعتبار:

• كيفية التخلي عن البرامج القديمة، النَادرة الاستخدام، والتي هي بحاجة للكثير من الرعاية.

• شراء البرامج التي تحتاجها فقط.

• تحقيق من النتائج المباشرة;
  في حال لم تكن البرامج القديمة التي تملكها تقدَّم لك أحدث التغييرات، النتائج والبيانات الدقيقة. قد يكون آن الأوان للبحث عما هو جديد.

• العائد على الاستثمار
  إستثمر أموال الإدارة في استبدال البرامج
replacing the old software if you expect it will facilitate the business process and save more money.

- **User requirements**
  If it delivers exactly what users are demanding. So spend some time to go through the requirements gathering process with your users.

- **Ease of use**
  Give serious consideration to ease of use for the end user and for your technical staff to deploy.

- **Compatibility**
  Before buying, ask searching questions to ensure maximum compatibility with your existing infrastructure.