Software Life-Cycle Management Guide
Revision 11/30/09

The Software Life-Cycle Management Guide is designed to help individual departments understand how OIT Site Licensing works and allow them to implement best practices for software acquisition and management as "One University," simplifying systems and processes. Because software is an asset of the University, it must be managed efficiently in order to protect the University. This guide provides a basic framework for software acquisition and sanitation, useful to all departments in the University. The aim is to promote aggregation of spend, reduction of the supplier base, and consolidation of products, where appropriate.

Contents

Licensing Software through OIT Site Licensing

1. OIT maintains a Site Licensing policy to drive the assessment of new purchases is required. Factors examined during licensing include:
   a. demand,
   b. acuteness of need,
   c. expected use,
   d. And budget for acquisition of new software.
      i. OIT's Site License Policy drives decisions and outlines determination of needs. See http://oit.osu.edu/site_license/slpolicy.html
2. OIT Site Licensing (OIT-SL) seeks to collaborate with and gather requirements from departments with an interest in the solution, to ensure that software determinations are made with full understanding of University need. Some examples of collaborative approaches include:
   a. request forms, such as
      i. The OIT Software Request form at http://oit.osu.edu/site_license/Software_LicRequest.pdf
   b. discussion on e-lists, such as
      i. DistCons <distcons@lists.acs.ohio-state.edu>
      ii. MacForum <macforum@lists.service.ohio-state.edu>
   c. meetings with groups, such as
      i. Site License Advisory Team
      ii. OSU Purchasing
      iii. CIO Advisory Community

iv.   Other interested departments
3. For products licensed to the site by OIT, or licensed by another entity and maintained by OI-SL, OIT will ensure that asset management guidelines are followed.
4. At renewal time, OIT-SL will lead an effort to determine continuing need for any products under license.
5. OIT-SL will seek to maximize savings through bulk purchases, extend training opportunities, and develop a central knowledgebase addressing common problems.
6. OIT-SL will manage the software lifecycle using the guide recommended to departments from acquisition to sanitation and retirement.

Managing Departmental Software Acquisitions

In the event that a piece of software is not licensed by OIT Site Licensing, individual departments that purchase a license for the software are responsible for ensuring that the software asset is managed properly.

Needs Assessment

1. If centrally licensed software cannot fulfill a need, checking against existing databases of other software products is recommended before a departmental purchase is made.
   a. OIT will begin maintaining a page listing scores and rankings of products that have been tested over time. This page may be viewed at: http://oit.osu.edu/site_license/slrankings.html
2. Needs Assessment must also include determining continuing need at renewal time.

Acquisition

(The ISO 27002 Security Framework has been adopted by the University, and contributes to this section.)

1. When acquiring software:
   a) software should be selected from a list of approved suppliers to encourage
      i.   savings through bulk purchase,
      ii. additional training opportunities,
      iii. broader knowledgebase development
   b) security requirements should be considered
   c) accessibility to people with disabilities should be considered
      i.   Departments may contact the Web Accessibility Center wac@osu.edu for testing accessibility of products.
   d) high priority should be given to reliability in the selection process
   e) Contractual terms should be agreed with suppliers.
2. The acquisition of products should be reviewed by staff who have the necessary skills to evaluate the implications, and approved by the business 'owner'.
3. Software licensing requirements should be met by obtaining adequate licenses for planned use and providing proof of ownership (eg via 'blanket' license agreements – one license covering a large number of software deployments – or retention of master disks/manuals).
4. Software is purchased and acquired when above standards are met.

Distribution

1. Prior to distribution, software should be tested to ensure:
   a. product is complete
   b. products work as described
   c. any instructions, including installation instructions, are as clear and concise as possible.
      i. Ensure the operation of the program is clear to all users, including persons with disabilities. If vendor-supplied instructions are not accessible to persons with disabilities, supplemental support should be provided.
2. Methods of distribution must be controlled as defined in licensing terms and conditions:
   a. Electronic distribution must be secured
      i. Distribution should be tied to a unique user ID in a database
   b. Over-the-counter or in-person distribution must also be secured.
      i. Distribution should be checked with photo ID against an electronic database.
3. Announcement of product should be:
   a. Clear and concise about terms, conditions, and use
   b. Detail relevant costs
   c. Describe value if applicable
4. See section on Compliance for information regarding EULAs and controls.

Asset Management

(The ISO 27002 Security Framework has been adopted by the University, and contributes to this section.)

1. Each software asset should be owned by a designated part of the organization.
   a) Owners are responsible for
      i. Ensuring that software is appropriately classified
         1. faculty, staff, students
         2. home use or OSU use
         3. consultant and third-party use
      ii. Defining and reviewing restrictions, classifications, and policies that surround the software.
2. Management of software should be divided into three roles, each owned by a different person or process:
   a) **Custodial** – The asset owner, in charge of maintaining inventory and determining classifications and restrictions for software.
      i. In OIT, this is the Site License Software Coordinator
      ii. In individual departments, this is generally a DNA or SLSC
   b) **Recording** – Classification of software distributed to individuals
      i. In OIT, the IT Service Desk fills the role of recording software distribution
      ii. Individual departments may have distribution points that fill this role
   c) **Authorization** – The approval process necessary to obtain and retire the software.
      i. OIT uses an electronic check against affiliation records to determine access to downloads and codes.

    ii. Individual departments can authorize users based on class rosters or academic fee payment.

3. Documented standards/procedures should be established for software inventory management that apply to the installation, which should cover the need to:

  a) record essential information about different types of software in an inventory

  b) meet software licensing requirements.

4. Software inventories should be:

  a) protected against unauthorized change

  b) checked periodically against actual assets (eg against physical assets or software licensing agreements to help identify gaps in registers and unauthorized copies of software)

  c) kept up-to-date

  d) independently reviewed.

5. Software inventories should specify:

  a) a unique identifier for each piece of software in use

  b) versions of hardware and software in use

  c) the location of software in use.

Compliance

(The ISO 27002 Security Framework has been adopted by the University, and contributes to this section)

1. Rules for the acceptable use of software assets should be identified, documented, and implemented.

2. All users of the software asset, including employees, students, contractors, and third-party users, are required to follow all terms and conditions relating to that software.

  a. If compliance with terms and conditions can be enforced electronically, they should be.

    i. Affiliation or enrollment status should be tied to University databases (e.g. SIS)

    ii. If compliance cannot be enforced electronically, it may be enforced through end user license agreements and/or through presentation of proof of affiliation or purchase (if required).

  b. Code control may be used, if licensing permits.

    i. Customers may be able to download software, but not activate it until a code is received.

  c. End user license agreements, if required, must be tracked and recorded in a secure database.

    i. Agreements may be paper or electronic

      1. Paper agreements should be recorded in an electronic database and housed off-site if possible

      2. Electronic agreement information should be backed up off site.

Sanitation and Retirement

1. Removal of software must occur after a relationship between user and University or area ends.

  a. Relationships may end when:

         i.   A customer disaffiliates with the University (employment termination, graduation, or other termination)
        ii.   A license agreement with a vendor is terminated.
  b. When a relationship ends, sanitation of software should begin immediately.
2. Destruction of master media and publications
  a. Media and publications should be destroyed in a manner that allows for tracking of destruction.
3. Maintenance of records
  a. Licensing agreements often indicate explicitly how long records must be kept after termination of the agreement.
        i.   University retention policies and software agreements should be used together to determine schedules.
  b. Place all records on a retention schedule upon termination of an agreement, in line with licensing agreement requirements or University retention policies.