# Software Acquisition and Usage Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

This document outlines the requirements for the acquisition and usage of software. It includes planning for and conducting evaluations of: (i) the software and, (ii) all necessary documentation, and related activities. Planning for and conducting the follow-up activities necessary to assure timely and effective resolution of problems will also be outlined.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions i.e. those people, elements or situations that are not covered by this policy or where special consideration may be made.

This policy applies to all software and support systems acquired or developed internally by [Company Name], as well as any software and support systems acquired, or developed by, an external corporate entity that subsequently merged with [Company Name].

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

1. **Open Source Software (OSS).** This is defined as software in which the source code is publicly available for use and/or modification.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. Employees may send informal recommendations to [insert eligible employee(s) here] if they identify software that fulfills a departmental or corporate need. The [insert eligible employee(s) here] is free to decline request for the suggested software for implementation if:
* The requirements gathering documentation listed in the Referenced Documents Section has been consulted, and the software does not conform to the policies listed therein.
* A substantial number of software products have been suggested.
* The software does not fulfill the needs of the department or the organization.
* The software does not meet the security requirements of the department or organization.
* A similar product has already been evaluated on the list of accepted products.
* [insert additional reasons here]
1. There are over 50 Open Source Software (OSS) licenses approved by the Open Source Initiative (OSI). In order to (a) minimize license management costs, (b) avoid litigation due to unanticipated license breaches, (c) ensure that existing commercial software can co-exist with any acquired OSS, and (d) protect any intellectual property that may arise [insert additional reasons here], [Company Name] will only acquire and deploy OSS that uses the licenses listed below. [Insert eligible employees(s)/office/position here] will not consider any OSS that uses other licenses.
* General Public License (GPL)
* GNU Library or “Lesser” General Public License (LGPL)
* MIT License (MIT)
* [insert additional licenses here]
1. Software shall be evaluated by [insert list of eligible employees here] in compliance with the company polices and needs. The employees must complete a software evaluation form for all software evaluated. The developers, or any other party responsible for the sale, marketing, or [insert any other activities] of the software product being acquired, are not allowed to perform either acquisition evaluations or acceptance testing. However, they are permitted to observe the process.
* Recognizing that current OSS evaluation tools have some shortcomings and are still immature, [Company Name] will employ a multifaceted best-practices approach to OSS evaluation that will include the use of more than one tool.
1. The following set of documentation should be evaluated before any software is acquired:

**The software development plan** (if acquiring custom developed software).

1. The [insert eligible employee(s) here] will evaluate the software development plan to be used for the project. The software developer must assure that:
* No other software plans exist for the project that have not been documented.
* The software development plans presented and evaluated comply with all stated policies and requirements.
* [insert additional requirements here]

**Other software documentation** (operating, user manuals, and other documentation).

1. The [insert eligible employee(s) here] will evaluate all other software documentation not identified in the preceding paragraph and ensure that:
* Each document adheres to the agreed format.
* Each document pertains to its stated software component.
* [Insert additional requirements here]
1. Software Evaluation Forms for each software acquisition evaluation must contain, at a minimum, the following items:

* Evaluation date
* List of participants
* Evaluation criteria used (e.g. performance, scalability, security)
* Evaluation results, including problems detected, as well as references to the software problem, as applicable
* Recommended corrective action
* [Insert additional items here]
1. All problems identified during acquisition evaluation and acceptance testing must be documented using the Software Evaluation Form. These problems are those that trigger non-conformance with any specified requirements. This documentation is to serve as a basis for the software developer to take corrective actions.
* Corrective actions will be evaluated to: verify that problems have been resolved; all changes have been implemented on the appropriate processes and products; and determine whether additional problems have been introduced.
1. The software acceptance checklist should contain, at a minimum, the following information:
2. The contact information for the employee(s)/officer/position listed in the Responsibility for Policy Compliance section
3. The developer’s or software manufacturer’s contact information
4. The software support information
5. Product information including:
* Product number
* Type of software
* License type
* [Insert other information here]
1. Type of user documentation included with the software e.g. user guide, online manual, an electronic help guide
2. System requirements, including:
* Minimum/recommended RAM
* Hard drive space
* Additional software required e.g. software libraries, databases
1. Beta testing results using the Software Evaluation Form
2. OSS allows software developers to freely modify the design and implementation of the application. [Company Name] anticipates that it [will/will not] modify any OSS acquired.
3. Software will not be acquired through user corporate credit cards, office supply, petty cash, or personal expense budgets. All software will be purchased through the [Purchasing/IT] department with approval and appropriate tracking provided by the [Software Asset Manager]. Acquisition channels will be restricted to ensure proper registration, inventory, and support information is recorded. Purchases made outside of the acceptable processes will not be reimbursed and will be removed from company computers.
4. Company-owned software may not be taken home and installed on employee-owned computers, unless permission is granted through a licensing agreement where the publisher has granted home-use licenses as part of the contract. [Company Name] commits to tracking any licenses installed for home use and monitoring use of media and software serial numbers to ensure only approved installations are completed.
5. Software will be used in accordance with the publisher’s license agreements and [Company Name’s] software use policy. All software, media, and documentation in use within [Company Name] belong to and are controlled by [Company Name].

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.