**OPEN SOURCE SOFTWARE POLICY**

**PURPOSE**

The use of free and open source software (FOSS) can provide efficient software solutions while significantly reducing development time, costs, and resources for [EMPLOYER'S NAME]. This policy ensures that FOSS is used properly and in compliance with software license obligations, mitigating potential legal liability and the risk of losing valuable proprietary rights.

Employees must adhere to the policies and procedures outlined below when acquiring, developing, using, copying, modifying, or distributing any software products or services on behalf of [EMPLOYER'S NAME].

This policy complies with all Vermont and federal laws and regulations.

Scope of policy

This policy applies to all employees during the course of their work, including interactions with third-party agents and vendors, when acquiring, developing, using, copying, modifying, licensing, or distributing any software that includes or is based on free and open source software. It governs the use of such software for all purposes, including internal operations, distribution to affiliates or third parties, or its incorporation into any products or services developed or offered by [EMPLOYER'S NAME].

**OPEN SOURCE REVIEW BOARD**

[EMPLOYER'S NAME]'s [Chief Information Officer/[DESIGNATED EXECUTIVE]] and FOSS Compliance Officer jointly oversee open source compliance as part of an Open Source Review Board (OSRB). Additional members may be appointed from IT, legal, operations, and management teams to support the company's software acquisition, use, development, and distribution activities.

The OSRB meets regularly, either in person or remotely, to fulfill its responsibilities under this policy. Meetings are scheduled as determined by the OSRB and outlined in advance, with a minimum frequency of once per [month/calendar quarter].

**FOSS PROCUREMENT**

Employees engaging third-party developers, vendors, or service providers to supply, maintain, or support software (including embedded software) or software services must adhere to the following requirements to ensure proper handling of FOSS:

Pre-contract requirements

* Approval rights: Contracts must reserve [EMPLOYER'S NAME]'s right to approve all FOSS components as a condition of agreement, including the right to use compliance tools to evaluate and approve each component.
* Disclosure obligations: Contracts must require providers to disclose all FOSS components as outlined in this policy.
* FOSS-free software: Providers must ensure software contains no unapproved FOSS components.
* Protections against liability: To the extent negotiable, contracts should include warranties, indemnities, and remedies that protect [EMPLOYER'S NAME] from infringement or other liabilities related to the use or distribution of FOSS.
* Maintenance and support: Providers must offer or identify reliable maintenance and support for all software, including FOSS components.

Pre-approval for FOSS use

For uses of FOSS not listed on the approved resource page [at [URL]/in Exhibit 1], employees must submit the following for review and approval:

* Required disclosures outlined in this policy.
* Intended uses of the FOSS or any software derived from it.
* Plans for redistribution of the FOSS or any derived products or services.

Third-party disclosure obligations

Before finalizing procurement agreements, ensure the provider commits to regularly providing the following:

* Names and version numbers of all FOSS components.
* Source of the FOSS, including any modified versions.
* Copies of all applicable licenses.
* Source code for the FOSS and any modifications.
* Copyright notices, attributions, acknowledgments, and product documentation.
* Contact information for maintenance and support providers, service descriptions, and terms.
* Summaries of interfaces, interactions, dependencies, and dependency charts for all FOSS components.

Waiver requests

To request a waiver for any disclosure requirements, employees must email [OSRB/[DEPARTMENT HEAD TITLE]] at [EMAIL ADDRESS], including:

* Details of the information unavailable.
* Reasons for its unavailability.
* Relevant facts for consideration.

**INTERNAL SOFTWARE DEVELOPMENT**

The [Software Development Manager/[TITLE]] overseeing each [EMPLOYER'S NAME] software development project must ensure comprehensive documentation of the project, including:

* Names of all contributors and participants involved in the project.
* Identification of all proprietary code developed for the project.
* Details of all FOSS used in or during the development process, including its name and version number.
* Titles and versions of applicable FOSS licenses.
* Description of how FOSS was used, including details of its integration with other software.
* Documentation of any modifications made to FOSS during development.
* Confirmation of all work-made-for-hire and intellectual property assignment agreements signed by contributors and participants, as required by their employment or supplier agreements [or the [EMPLOYER'S NAME] Employee Handbook].

**THIRD PARTY DISTRIBUTION**

For any distribution of FOSS outside [EMPLOYER'S NAME], adhere to the following guidelines:

Approval for distribution

* Distribution or licensing of FOSS, including its use in the development of [EMPLOYER'S NAME] products or services, must be submitted to [DEPARTMENT HEAD TITLE] for review and written approval.
* No FOSS, including copies or modifications made by or for [EMPLOYER'S NAME], may be distributed or shared with customers, third parties, or FOSS communities without prior approval.

Agreement compliance

* Any agreements for licensing or distribution of FOSS must align with [EMPLOYER'S NAME]'s standard outbound software license agreement.
* The terms must be reviewed and approved by [DEPARTMENT HEAD TITLE] in consultation with the company’s legal counsel.

Customer documentation

* Customers and third parties must receive:
	+ A copy of the approved Software License Agreement.
	+ A copy of the governing FOSS license or instructions on how to obtain it if additional terms apply.

**RESPONSIBILITIES OF [DEPARTMENT HEAD TITLE]**

The [DEPARTMENT HEAD TITLE], [in coordination with/under the direction of] the [FOSS Compliance Officer/[DEPARTMENT HEAD TITLE]], oversees the following activities:

Approval management

* Review and process all requests for the approval of FOSS to be acquired, used, developed, modified, distributed, or otherwise made available by [EMPLOYER'S NAME].
* Decide on the permissibility of proposed FOSS activities after evaluating legal, data security, software architecture, and commercial factors.
* Communicate decisions and approvals in writing (including electronically) to the employees responsible for the proposed FOSS activity.

FOSS resource management

* Maintain an up-to-date list of pre-approved FOSS, published [on the FOSS Resource Page at [URL]/in Exhibit 1], including:
	+ Name and version number.
	+ Governing license.
	+ Approved uses, including any permissible copying or modifications.
	+ Required conditions and restrictions.
	+ Permissible external distribution and related conditions or restrictions.

Compliance coordination

* Work with the [Chief Information Officer (CIO)/OTHER EXECUTIVE] and [Law Department/legal counsel] to:
	+ Ensure compliance with all inbound FOSS license terms through appropriate procedures.
	+ Develop and publish standard FOSS outbound license terms on the FOSS Resource Page for employee use in proposed distribution submissions.

Additional responsibilities of [DEPARTMENT HEAD TITLE]

In addition to overseeing FOSS approval procedures, the [DEPARTMENT HEAD TITLE] is tasked with the following duties, either collectively or through the FOSS Compliance Officer or designated members:

*Communication and education*

* Engaging with product managers, software developers, and third-party providers to ensure they understand and comply with this policy and applicable FOSS license requirements.
* Responding to questions and communications related to [EMPLOYER'S NAME]'s use of FOSS.

*Monitoring and reporting*

* Maintaining records and responding to reports of suspected non-compliance, including the use of unapproved, unlicensed, or defective FOSS on company systems or devices.

*Policy development and training*

* Creating additional practices and procedures and providing employee training to ensure compliance with this policy and protection of [EMPLOYER'S NAME]'s intellectual property rights.

*Automated tools and pre-launch reviews*

* Selecting and overseeing the use of automated tools to detect and manage FOSS compliance, scanning all products and services prior to launch for FOSS presence and license terms.

*FOSS audits*

* Conducting or overseeing periodic audits of software on company systems to:
	+ Communicate audit findings, license requirements, and potential risks to responsible employees.
	+ Recommending alternatives or modifications to mitigate adverse effects of FOSS usage.
	+ Notifying legal counsel and escalate decisions regarding activities that may compromise intellectual property rights.

*Enforcement and remediation*

* Monitoring adherence to this policy and taking corrective actions to address and mitigate non-compliance.

*Record keeping*

* Maintaining detailed records of audits, decisions, and communications with internal and external stakeholders*.*

*Legal consultation and escalation*

* Consulting legal counsel for issues involving FOSS usage and escalating matters to executive management when necessary.

*Reporting and leadership*

* Providing periodic updates to the [Board of Directors/[COMMITTEE OR OTHER BODY]] to ensure policy alignment with company goals and strategies.

**REPORTING FOSS NON-COMPLIANCE**

Employees must immediately report any suspected non-compliance related to FOSS on [EMPLOYER'S NAME]'s networks, systems, or devices to the [FOSS Compliance Officer/OSRB/[DEPARTMENT HEAD TITLE]]. Relevant situations include:

* Use of unlicensed FOSS.
* Installation or use of FOSS not approved under this policy.
* FOSS that presents security risks, contains material defects, or includes malicious code.

Reports should include all pertinent documents and information related to the issue.

**MERGERS AND ACQUISITIONS**

Prior to any merger or acquisition, the FOSS Compliance Officer, in collaboration with the [DEPARTMENT HEAD TITLE] and [EMPLOYER'S NAME]'s legal counsel, must conduct a due diligence review of the target entity's FOSS activities. This assessment should align with the objectives and procedures outlined in this policy to identify potential risks and ensure compliance.

**CONSEQUENCES FOR NON-COMPLIANCE**

Violations of this policy may result in disciplinary action, up to and including termination of employment.

**APPLICABILITY TO COLLECTIVE BARGAINING AGREEMENTS**

The terms outlined in this policy are designed to complement, not replace, amend, or supplement, the terms and conditions of employment outlined in any collective bargaining agreement that applies to unionized employees at [EMPLOYER'S NAME].

Employees covered by a collective bargaining agreement should refer to its terms for guidance. Where this policy's terms differ from those in the applicable collective bargaining agreement, the agreement's terms will take precedence.

**ACKNOWLEDGEMENT OF RECEIPT AND REVIEW**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (employee name), acknowledge that on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date), I received and reviewed a copy of [EMPLOYER'S NAME]’s [NAME OF POLICY]. I understand that it is my responsibility to familiarize myself with the policy and adhere to its terms.

I also acknowledge that this policy is not intended to create an employment contract or alter my at-will employment status, unless otherwise specified in a written agreement signed by an authorized representative of [EMPLOYER'S NAME]. Any delay or failure by [EMPLOYER'S NAME] to enforce the provisions of this policy does not constitute a waiver of its rights to enforce them in the future.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

**[EXHIBIT 1]**

[INSERT]