**Reference Free and Open Source Software Policy**

**for Financial Services Institutions**

**Version 0.2.2**

**Fintech Open Source Foundation (FINOS)**

**Open Source Readiness Program**

**Disclaimer**: This is a template for a comprehensive free and open source software (FOSS) policy for a financial services institution, including sample provisions governing the acquisition and use of FOSS, and contribution to FOSS projects. It is offered only as a reference, not as a complete policy or as legal advice. While this policy has been drafted to be generally applicable, it does not define every implementation detail. Every company's policy should be customized to its particular needs, policy and technical environments, and risk tolerance.

© 2017 Fintech Open Source Foundation. This document is licensed under the terms of the Creative Commons Attribution (CC By) License, version 4.0 (<https://creativecommons.org/licenses/by/4.0/>). It is offered as-is and as-available, without representation or warranty of any kind, whether express, implied, statutory, or other. The original version of this document is available at TKTKTK. Any modified version must indicate modifications. This notice and disclaimer must be retained on any copies and derivative works.

# Overview & Purpose

It is the policy of [Company Name] (“Company”) to use, contribute to, and publish Free and Open Source Software (“FOSS”) when doing so furthers Company’s business purposes and does not present unacceptable risks. This Free and Open Source Software Policy (the “Policy”) describes the requirements that Company personnel must observe when incorporating FOSS into a Company software product, distributing FOSS to third parties, contributing code and other materials to third-party FOSS projects, publishing Company software products as FOSS, and otherwise interacting with the FOSS community.

There are many potential benefits to using and contributing to FOSS. Effective participation in FOSS ecosystems can lower software development costs, increase the pace of software development, improve software quality and security, and promote developer recruitment and retention. As with any undertaking, engagement with FOSS raises questions about avoidable risks. These include inadvertently disclosing sensitive information, giving up exclusive rights to intellectual property, infringement of third party rights, introduction of security vulnerabilities to Company software products, and reputational harm.

This policy is intended to minimize these risks, comport with the recommendations of the Federal Financial Institutions Examinations Council,[[1]](#footnote-1) and to ensure that, in using and contributing to FOSS, the Company and its employees respect the rights of third parties, comply with applicable regulations, and engage productively with the FOSS community.

# Authority

To the extent this Policy implicates the exclusive authority of the Board of Directors to take certain actions, such as to authorize the licensing of Company intellectual property rights, that authority is expressly delegated to the Chief Technology Officer, to be exercised consistent with the limitations set forth herein.

# Scope

## Applicability

This Policy applies to all Company employees, contractors, and consultants, worldwide. It governs all use of FOSS, modified or unmodified, including when the FOSS is: installed or used on Company computers; incorporated into Company Software Products; distributed (alone or together with Software Products) to customers or other third parties; published by the Company; or contributed (as modifications or original software) to a third-party FOSS Project or organization.

## Pre-Existing Use of FOSS

The FOSS Review Board (FRB) shall establish a process for ensuring, within a reasonable period of time after this Policy is adopted, that all existing Company use of FOSS initiated before the adoption of this Policy complies with the requirements of this Policy.

Best Practice – Pre-Existing FOSS Compliance Procedures

1. The FRB should produce an inventory of existing FOSS use by surveying Product Owners, using automated scanning tools, and other means. It should then review this inventory to identify any inconsistencies with this Policy.
2. When a Product Team updates a preexisting FOSS component to a new version, or makes modifications to a preexisting FOSS component, the updated or modified component is subject to the policies and procedures applicable to new uses or modifications of FOSS.

# Roles and Responsibilities

Company shall establish a **FOSS Review Board (“FRB”)** upon adoption of this Policy. At a minimum, the FRB shall include representatives from Legal, Security, and Software Architecture. The FRB shall meet or communicate as frequently as necessary to carry out its responsibilities expeditiously. The FRB shall have the following responsibilities:

1. Develop and communicate Company FOSS strategy in consultation with Company’s technical and corporate leadership;
2. Establish implementing procedures for this Policy;
3. Review and make determinations on FOSS Requests; and
4. Periodically collect feedback about and review this Policy, then make appropriate recommendations for revising it.
5. Provide support, training, and documentary materials that enable compliance with this policy.

**Compliance** shall work with the FRB as necessary to develop procedures to implement this Policy, to design and conduct any required training, and to resolve questions regarding the interpretation of this or other Company policies.

**Legal** shall participate in the FRB. It shall review all FOSS Licenses referenced in FOSS Requests and applicable to pre-existing FOSS and shall work with the FRB to develop and communicate compliance requirements for each.

**Security** shall participate in the FRB. It shall establish any necessary procedures for identifying and addressing security vulnerabilities in FOSS components, and shall work with the FRB and Product Teams to notify affected parties of and remediate known security issues in FOSS components.

# Implementation

The FRB shall be responsible for implementation of this Policy and shall have discretion to determine what procedures are necessary to implement it consistent with the Policy’s requirements.

Best Practice – Implementation Procedures

The FRB should produce:

1. A FOSS License List (or database) identifying each FOSS License reviewed by the FRB and recording:
   1. the name and version of the license reviewed;
   2. a link or reference to the full text of the license;
   3. license compliance requirements, determined by the FRB, including requirements specific to modification or distribution of the FOSS;
   4. which types of use (e.g. consumption, modification, distribution, or network connection) require additional compliance considerations; and
   5. which uses are subject to pre-approval, which require FRB review, and which are prohibited under all circumstances.
2. A FOSS Training Program, and accompanying materials, that employees must complete before being authorized to make new FOSS Use or Contribution Requests. The training program should cover, at a minimum, the following topics:

* Software intellectual property basics
* Common FOSS licenses and compliance requirements
* Risk factors related to FOSS use, modification, and contribution
* The requirements of this Policy and any associated procedures
* Proper Source Control Management (SCM) system usage for use of FOSS in Software Products
* FOSS community norms and best practices
* Applicability of the Company’s employee code of conduct to interactions with FOSS Projects and communities

# FOSS Training Policy

The FRB shall develop a FOSS Training Program to communicate the requirements of this Policy to employees to which it applies and shall work with Compliance to conduct trainings.

Best Practice – FOSS Training Procedures

Beginning 90 days after adoption of this Policy, each Company employee must attest that they have read and understood the Policy before submitting any FOSS Request or being authorized to modify any internal software repository containing FOSS source code. Employees should also complete the FOSS Training Program before or as soon as practicable after submitting any FOSS Request or being authorized to modify any internal software repository containing FOSS source code.

# FOSS Use Policy

The FRB shall develop procedures governing the use of FOSS, designed to promote the Company’s FOSS strategy, compliance with regulations and obligations to third parties, and the security of Company Software Products incorporating FOSS. These procedures shall cover all use of FOSS, including: installation or use on employee workstations and Company servers; incorporation of FOSS into Company Software Products; and distribution of FOSS to customers and third parties.

Best Practice – FOSS Use Procedures

1. FOSS Request Process. Each FOSS use is subject to the following process:
   1. FOSS Use Report. The employee or Project Team wishing to use a FOSS component shall submit to the FRB, via the FOSS Request System, a FOSS Use Report including the following information:
      1. Information about the FOSS component:
         1. Name
         2. Version
         3. Origin URI
         4. Applicable FOSS license(s)
         5. Any additional license requirements or exceptions
         6. Brief description of component’s purpose
      2. Information about the proposed use of the FOSS component:
         1. Requesting employee or Project Team
         2. The Company Software Product (if any) the Report relates to
         3. Brief description of use and its context
         4. Description of combinations or interactions with Software Products
         5. Whether the FOSS component has been or will be modified
         6. A summary of any modifications
         7. Whether the FOSS will be distributed outside Company
      3. Whether the FOSS License List identifies the proposed use as pre-approved for the component’s FOSS License.
   2. Security Review. The FOSS component shall be reviewed for vulnerabilities.
      1. The review shall be conducted according to standards promulgated by Security defining which tools must be used for automated security reviews, when review by Security is necessary, and when a third-party audit is required.
      2. The security review shall include consultation of the National Vulnerabilities Database (<https://nvd.nist.gov>) for any listed vulnerabilities.
      3. The Project Team must fix any critical vulnerabilities and any other vulnerabilities required by Security before the use may be approved.
   3. FRB Review. If the proposed use is not pre-approved, the FRB shall:
      1. Identify the applicable FOSS License(s) and any other terms.
      2. Perform a risk analysis of the proposed use, consisting of:
         1. Identifying any significant legal, financial, reputational, security, or strategic risks;
         2. Identify any risk-mitigating measures that should be taken if the use should be approved.
      3. Approve or reject the FOSS Use Report and update the request to indicate its decision.
         1. If the request is approved, the FRB should include with its approval any applicable compliance and risk-mitigation instructions particular to the proposed use. The FOSS component shall then be made available to the Project Team via an Approved Channel.
         2. FRB approval is limited to the version identified in request. If the FOSS component is later upgraded or modified, a new FOSS Use Report must be submitted. If the FOSS License for the component has not changed, the new version shall be subject to any pre-approval applicable to the preceding use.
2. Compliance. Once a FOSS Use Report is approved, the Project Team must observe the following requirements:
   1. FOSS source code files must be maintained separately from non-FOSS source code in a Source Code Management (SCM) system. (I.e. source code may not be copied from FOSS files into non-FOSS files, and FOSS files may not be copied into directories containing non-FOSS files.)
   2. Project Team must implement all compliance & risk mitigation requirements identified in the FOSS License List and by the FRB.
3. Maintenance.
   1. Security shall monitor vulnerability notifications for each FOSS component in use at Company and shall notify Project Teams of vulnerabilities in the FOSS components they are using.
   2. When a critical security vulnerability is identified, the Project Team must promptly upgrade to a patched version (if available) or implement any mitigating actions required by Security.
   3. If the FOSS component has been distributed to customers or third parties, the FRB shall arrange for appropriate notice and remediation support to be provided to any recipients that can reasonably be identified.

# FOSS Modification Policy

The FRB shall develop procedures governing the modification of FOSS by employees. In addition to the priorities identified in the preceding section governing FOSS use (strategy, compliance, and security), these procedures should promote the documentation of all Company modifications to FOSS and the contribution of modifications to upstream FOSS Projects where appropriate and consistent with Company’s FOSS strategy and all applicable FOSS Licenses. These procedures shall cover all modifications to FOSS, whether intended for use internally, or with hosted or distributed Company Software Products.

Best Practice – FOSS Modification Procedures

1. Modification Process. The process for making modifications to third-party FOSS is as follows:
   1. Request. A Project Team modifying a third-party FOSS component must submit a new FOSS Use Report to the FRB, including details about the nature and purpose of the proposed modifications. No modifications may be used in production, distributed, or contributed outside the Company until the request is approved.
   2. FRB Determination. The FRB shall review and approve or reject the FOSS Use Report according to the procedures implementing the FOSS Use Policy.
   3. Making the Modifications.
      1. Modifications must be tracked using an SCM system so that the differences from the baseline FOSS component’s source readily identifiable. The SCM system must capture the identity of any employee making Contributions accurately in a manner consistent with Company’s internal audit requirements.
      2. If required by the applicable FOSS License(s), the Project Team must include appropriate notice in the source code stating that the FOSS has been modified and, if required, describing the modifications.
   4. Building the Modified FOSS. If applicable, the modified FOSS component should be built using standard tools. If a custom process or custom tools are required, the Project Team must provide the infrastructure team documentation on the process, tools, and their maintenance.
2. Compliance. Modifications to FOSS are subject to the compliance requirements described in the FOSS Use Procedures, as well as any additional requirements applicable to modifications, as identified by the FRB or the applicable FOSS License.
3. Maintenance. The modified FOSS is subject to the maintenance requirements described in the FOSS Use Procedures. When contributing the modifications to the originating FOSS Project would ease maintenance and be consistent with Company’s FOSS strategy, Project Teams should be encouraged to submit a FOSS Contribution Request.

# FOSS Contribution and Publication Policy

The FRB shall develop procedures governing (i) employee Contributions of code and other materials to third-party FOSS Projects and (ii) publication of Company Software Products under FOSS Licenses. These procedures should promote the strategic, compliance, and security priorities identified in the FOSS Use Policy.

Best Practice – FOSS Contribution and Publication Procedures

All employee Contributions to third-party FOSS Projects must be approved in advance by the FRB, either specifically or because it is pre-approved. Likewise, any publication of a Company Software Product, in whole or in part, under a FOSS License, must be approved in advance by the FRB.

If a proposed Contribution consists of modifications to an existing third-party FOSS Project, those modifications must be approved as described in the FOSS Modification Procedures before the FOSS Contribution Request may be approved.

1. Contribution Request Process.
   1. FOSS Contribution Request. The Project Team must submit a FOSS Contribution Request via the FOSS Request System, including the following information:
      1. If the proposed Contribution consists of modifications to a third-party FOSS Project:
         1. a link to the approved FOSS Use Report; and
         2. links to information about the FOSS Project’s contribution requirements, including any contributor license agreements.
      2. If the proposed Contribution is of a Company Software Product (in whole or in part):
         1. The name and version (if applicable) of the Software Product;
         2. A description of the Contribution’s functionality;
         3. The Contribution’s relationship to any Company Software Products;
         4. A list of the Contribution’s dependencies, including on FOSS, third-party proprietary, and Company proprietary components; and
         5. The location of the internal SCM repository where the proposed Contribution is maintained.
      3. The Project Team’s rationale for the Contribution, including a description of any associated benefits and risks.
      4. The proposed contributors, including their names and (if applicable) the GitHub ID or other account under which they will make the Contribution.
   2. FOSS Review Board review. The FRB will review the FOSS Contribution Request and make a determination. In evaluating a request, the FRB must consider the following risk factors:
      1. The potential impact on proprietary Company intellectual property, including any:
         1. Reciprocal (i.e. copyleft) licensing requirements in the applicable FOSS License(s);
         2. Trade secrets that may be divulged as a result of the Contribution; or
         3. Patented or patentable inventions that may be published or licensed as a result of the Contribution.
      2. Improper disclosures, including of:
         1. Third-party proprietary source code or other materials;
         2. Materials restricted by non-disclosure agreements and similar covenants;
         3. Personally identifiable information of customers, employees, or others;
         4. Other regulated information; or
         5. Sensitive company data, including private keys, passwords, or proprietary datasets.
      3. The potential impact on the competitiveness of any Company Software Product.
      4. The potential impact on existing or prospective revenue sources, including from software licensing.
      5. The potential for reputational harm, including from issues with the contributed materials, the Company’s subsequent interactions with the FOSS community, and similar issues.
   3. FRB Approval. When the FRB approves a request, it may optionally pre-approve related future Contributions, subject to appropriate scope limitations. For example, it may approve future Contributions to the same third-party FOSS Project that constitute bug fixes, or that do not include separately-produced Company code or other materials. The FRB may also limit the scope of pre-approvals by time, by Project Team, or otherwise as it deems appropriate.
2. Pre-Contribution Requirements.
   1. Development. A proposed Contribution must be prepared in an internal SCM tool.
   2. Legal.
      1. Any contributor license agreement or other legal attestation required for contributors to the FOSS Project must be reviewed and approved by Legal (unless Contributions to the FOSS Project have been previously approved and no additional signatures/approvals are required).
      2. All intellectual property rights in the Contribution that are held by any Company entity must be transferred to the Contributing Entity.
   3. Attribution. The Contribution must identify the company as the Contribution’s copyright owner, where and as appropriate. The Project Team members may be credited as the developers, where and as appropriate.
   4. Compliance. The Contribution must comply with the FOSS Project’s policies, procedures, and codes of conduct, as well as with Company policy. If there is a conflict among these, the contributor must seek a resolution from the FRB before proceeding.
   5. Peer Review. After the FRB has approved a proposed Contribution and before the Contribution is made, it must be reviewed by a developer or manager familiar with this Policy. The peer reviewer must determine that the Contribution:
      1. does not include any Company IP not approved by the FRB for Contribution;
      2. does not include any confidential Company or third-party information;
      3. does not include any other sensitive information;
      4. includes any compliance information required by the FOSS License List or FRB;
      5. includes any required Company notices;
      6. conforms to the Company’s code of conduct and policies for FOSS Contributions; and
      7. is consistent with the FOSS Project’s policies and code of conduct.
3. Contribution. Contributions to public source code repositories must be made from a user account (e.g. GitHub ID) associated with the contributing Project Team member in the FOSS Records System. Any copyright attribution must be to the Company.
4. Publication of Company Software Products. Any publication of a Company Software Product under a FOSS License is subject to the above requirements applicable to Contributions. In addition, before publication of the Company Software Product, Finance must determine whether any corresponding adjustment should be made to the Company books, for example to reduce the investment cost of the Company Software Product. It must then make any such adjustment before the Company Software Product may be published.
5. Individual (“off-the-clock”) Contributions. If an employee produces a Contribution on their own time and with their own hardware and resources, and that does not constitute company property under the employee’s IP assignment agreement, the Contribution is governed by the Outside Business Dealings policy and subject to any applicable approvals thereunder. Such Contributions should be made in the employee’s own name and without reference to the Company.

# General

## Exceptions. Any exception to this Policy must be made in writing and approved by the FRB.

## Questions. Any questions regarding compliance with this Policy should be directed to the FRB.

## Ownership. This Policy is owned by the FRB.

## Related Policies. The following Company policies may also be applicable to various aspects of the use, modification, contribution, and publication of FOSS as described in this Policy and associated procedures:

## Code of Conduct

## Intellectual Property

## Technology Acquisition

## Social Media

## Business Process Change Management

## Information Security

## Information Classification

## Electronic Communications

## Software Development & Maintenance

## Software and IT Infrastructure Development Lifecycle

## Source Control Management

## Secure Coding

# Definitions

As used in this Policy and associated procedures, the following terms have the meanings given below:

## Approved Channel: A software acquisition channel providing access to software artifacts approved by Company for use in Software Products.

## Company Software Product: Software originally developed wholly or primarily by Company.

## Contribution: Materials (including software source code, documentation, media assets, and other digital content) submitted for inclusion in a FOSS Project.

## Contributing Entity: The Company entity or affiliate that effects a Contribution.

## Free and Open Source Software (FOSS): Software (including source code, executable files, documentation, media assets, and other digital content) licensed under the terms of a FOSS License.

## FOSS License: A license listed as an Open Source License by the Open Source Initiative (<https://opensource.org/licenses/>) or as a Free Software License by the Free Software Foundation (<https://www.gnu.org/licenses/license-list.en.html>).

## FOSS Project: A collaborative software-development effort undertaken by one or more individuals or entities.

## FOSS Request: A FOSS Use Report or FOSS Contribution Request.

## FOSS Contribution Request: A request by an employee or Project Team to make a Contribution to an external FOSS Project or to publish a Software Product as FOSS.

## FOSS Use Report: A request by an employee or Project Team to use third-party FOSS on Company hardware or incorporate third-party FOSS into a Software Product.

## FOSS Request System: An internal system for submitting, discussing, and resolving FOSS Requests.

## FOSS Review Board: The interdepartmental committee defined in Section 4(A) of this Policy.

## FOSS Training Program: The training program described by Section 5 of this Policy.

1. “[Risk Management of Free and Open Source Software](https://www.fdic.gov/news/news/financial/2004/fil11404a.html)” issued by the Federal Financial Institutions Examination Council (FFIEC), October 2004. [↑](#footnote-ref-1)