Reference Free, Libre, and Open Source Software Policy
for Financial Services Institutions

Version 0.2.3

Fintech Open Source Foundation (FINOS)
Free Software Readiness Program

Disclaimer: This is a template for a comprehensive free, libre, and open source software (FLOSS) policy for a financial services institution, including sample provisions governing the acquisition and use of FLOSS, and contribution to FLOSS 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.

1. Overview & Purpose

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

There are many potential benefits to using and contributing to FLOSS. Effective participation in FLOSS 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 FLOSS 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] and to ensure that, in using and

1 "Risk Management of Free and Open Source Software" issued by the Federal Financial Institutions Examination Council (FFIEC), October 2004.

contributing to FLOSS, the Company and its employees respect the rights of third parties, comply with applicable regulations, and engage productively with the FLOSS community.

2. 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 / Group CTO / CIO], to be exercised consistent with the limitations set forth herein.

3. Scope

A. Applicability

This Policy applies to all Company employees, contractors, and consultants, worldwide. It governs all use of FLOSS, modified or unmodified, including when the FLOSS 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 FLOSS Project or organization.

B. Pre-Existing Use of FLOSS

The FLOSS 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 FLOSS initiated before the adoption of this Policy complies with the requirements of this Policy.

Best Practice – Pre-Existing FLOSS Compliance Procedures

1) The FRB should produce an inventory of existing FLOSS 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 FLOSS component to a new version, or makes modifications to a preexisting FLOSS component, the updated or modified component is subject to the policies and procedures applicable to new uses or modifications of FLOSS.

1. Roles and Responsibilities

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

A. Develop and communicate Company FLOSS strategy in consultation with Company’s technical and corporate leadership;
B. Establish implementing procedures for this Policy;

C. Review and make determinations on FLOSS Requests; and
D. Periodically collect feedback about and review this Policy, then make appropriate recommendations for revising it.
E. Arrange to 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 FLOSS Licenses referenced in FLOSS Requests and applicable to pre-existing FLOSS 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 FLOSS components, and shall work with the FRB and Product Teams to notify affected parties of and remediate known security issues in FLOSS components.

1. 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

1) Supporting Materials. The FRB should produce (or obtain):

a. A FLOSS License List (or database) identifying each FLOSS License reviewed by the FRB and recording:

i) the name and version of the license reviewed;

ii) a link or reference to the full text of the license;

iii) license compliance requirements, determined by the FRB, including requirements specific to modification or distribution of the FLOSS;

iv) which types of use (e.g. consumption, modification, distribution, or network connection) require additional compliance considerations; and

v) which uses are subject to pre-approval, which require FRB review, and which are prohibited under all circumstances.

b. A FLOSS Training Program, and accompanying materials, that employees must complete before being authorized to make new FLOSS Use or Contribution Requests. The training program should cover, at a minimum, the following topics:

i) Software intellectual property basics

ii) Common FLOSS licenses and compliance requirements

iii) Risk factors related to FLOSS use, modification, and contribution

iv) The requirements of this Policy and any associated procedures

v) Proper Source Control Management (SCM) system usage for use of FLOSS in Software Products

vi) FLOSS community norms and best practices

vii) Applicability of the Company's employee code of conduct to interactions with FLOSS Projects and communities

2) Pre-Approval of FLOSS Requests.

a. To ensure the timely processing of requests, the FRB should define categories of pre-approved requests that do not require individual review. Generally, the FRB should pre-approve categories of FLOSS Requests that are likely to present little or no risk to the Company.

b. Pre-approvals may be limited in scope as appropriate to limit risk. A pre-approval's scope may be limited to a particular time period, FLOSS component, Project Team, type of request, or any other criteria or combination of criteria that the FRB deems appropriate. Examples of scope-limited pre-approvals might include:

i) All contributions to third-party Project A, a non-business critical library;

ii) Bug fixes and security patches to any third-party project with an approved FLOSS License;

iii) Contributions by Project Team 1 to third-party Project B related to Internal Project 1A; etc.

1. FLOSS Training Policy

The FRB shall develop a FLOSS 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 – FLOSS 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 FLOSS Request or being authorized to modify any internal software repository containing FLOSS source code. Employees should also complete the FLOSS Training Program before or as soon as practicable after submitting any FLOSS Request or being authorized to modify any internal software repository containing FLOSS source code.

2. FLOSS Use Policy

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

Best Practice – FLOSS Use Procedures

1) FLOSS Request Process. Each FLOSS use is subject to the following process:

a. FLOSS Use Report. The employee or Project Team wishing to use a FLOSS component shall submit to the FRB, via the FLOSS Request System, a FLOSS Use Report including the information below. (If the FLOSS component has been preapproved for the proposed use, some or all of this information may be pre-filled by the system.)

i. Information about the FLOSS component:

1. Name

2. Version

3. Origin URI

4. Applicable FLOSS license(s)

5. Any additional license requirements or exceptions

6. Brief description of component's purpose

ii. Information about the proposed use of the FLOSS 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 FLOSS component has been or will be modified

6. A summary of any modifications

7. Whether the FLOSS will be distributed outside Company

iii. Whether the FLOSS License List identifies the proposed use as pre-approved for the component's FLOSS License.

b. Security Review. The FLOSS component shall be reviewed for vulnerabilities.

i. 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.

ii. The security review shall include consultation of the National Vulnerabilities Database (https://nvd.nist.gov) for any listed vulnerabilities.

iii. The Project Team must fix any critical vulnerabilities and any other vulnerabilities required by Security before the use may be approved.

c. FRB Review. If the proposed use is not pre-approved, the FRB shall:

i. Identify the applicable FLOSS License(s) and any other terms.

ii. 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.

iii. Approve or reject the FLOSS 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 FLOSS 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 FLOSS component is later upgraded or modified, a new FLOSS Use Report must be submitted. If the FLOSS 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 FLOSS Use Report is approved, the Project Team must observe the following requirements:

a. FLOSS source code files must be maintained separately from non-FLOSS source code in a Source Code Management (SCM) system. (I.e. source code may not be copied from FLOSS files into non-FLOSS files, and FLOSS files may not be copied into directories containing non-FLOSS files.)

b. Project Team must implement all compliance & risk mitigation requirements identified in the FLOSS License List and by the FRB.

3) Maintenance.

a. Security shall monitor vulnerability notifications for each FLOSS component in use at Company and shall notify Project Teams of vulnerabilities in the FLOSS components they are using.

b. 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.

c. If the FLOSS 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.

1. FLOSS Modification Policy

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

Best Practice – FLOSS Modification Procedures

1) Modification Process. The process for making modifications to third-party FLOSS is as follows:

    a. Request. A Project Team modifying a third-party FLOSS component must submit a new FLOSS Use Report to the FRB, including details about the nature and purpose of the proposed modifications. If the proposed modifications are not pre-approved, they must be approved by the FRB before they may be used in production, distributed, or contributed outside the Company.

    b. FRB Determination. The FRB shall review and approve or reject the FLOSS Use Report according to the procedures implementing the FLOSS Use Policy. The FRB should maintain a policy, available to Project Teams, stating the expected review time for FLOSS Use Reports.

    c. Making the Modifications.

        i. Modifications must be tracked using an SCM system so that the differences from the baseline FLOSS 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.

        ii. If required by the applicable FLOSS License(s), the Project Team must include appropriate notice in the source code stating that the FLOSS has been modified and, if required, describing the modifications.

d. Building the Modified FLOSS. If applicable, the modified FLOSS 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 FLOSS are subject to the compliance requirements described in the FLOSS Use Procedures, as well as any additional requirements applicable to modifications, as identified by the FRB or the applicable FLOSS License.

3) Maintenance. The modified FLOSS is subject to the maintenance requirements described in the FLOSS Use Procedures. When contributing the modifications to the originating FLOSS Project would ease maintenance and be consistent with Company's FLOSS strategy, Project Teams should be encouraged to submit a FLOSS Contribution Request.

1. FLOSS Contribution and Publication Policy

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

Best Practice – FLOSS Contribution and Publication Procedures

All employee Contributions to third-party FLOSS 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 FLOSS License, must be approved in advance by the FRB.

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

1) Contribution Request Process.

a. FLOSS Contribution Request. The Project Team must submit a FLOSS Contribution Request via the FLOSS Request System, including the following information:

i. If the proposed Contribution consists of modifications to a third-party FLOSS Project:

1. a link to the approved FLOSS Use Report; and

2. links to information about the FLOSS Project's contribution requirements, including any contributor license agreements.

ii. 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 FLOSS, third-party proprietary, and Company proprietary components; and

5. The location of the internal SCM repository where the proposed Contribution is maintained.

iii. The Project Team's rationale for the Contribution, including a description of any associated benefits and risks.

iv. The proposed contributors, including their names and (if applicable) the GitHub ID or other account under which they will make the Contribution.

b. FLOSS Review Board review. The FRB will review the FLOSS Contribution Request and make a determination. In evaluating a request, the FRB must consider the following risk factors:

i. The potential impact on proprietary Company intellectual property, including any:

1. Reciprocal (i.e. copyleft) licensing requirements in the applicable FLOSS 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.

ii. 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.

iii. The potential impact on the competitiveness of any Company Software Product.

iv. The potential impact on existing or prospective revenue sources, including from software licensing.

v. The potential for reputational harm, including from issues with the contributed materials, the Company's subsequent interactions with the FLOSS community, and similar issues.

c. FRB Approval. When the FRB approves a request, it should consider whether to pre-approve similar or related requests, as provided for in Section 5(2) above.

2) Pre-Contribution Requirements.

a. Development. A proposed Contribution must be prepared in an internal SCM tool.

b. Legal.

i. Any contributor license agreement or other legal attestation required for contributors to the FLOSS Project must be reviewed and approved by Legal (unless Contributions to the FLOSS Project have been previously approved and no additional signatures/approvals are required).

ii. All intellectual property rights in the Contribution that are held by any Company entity must be transferred to the Contributing Entity.

c. 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.

d. Compliance. The Contribution must comply with the FLOSS 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.

e. 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:

i. does not include any Company IP not approved by the FRB for Contribution;

ii. does not include any confidential Company or third-party information;

iii. does not include any other sensitive information;

iv. includes any compliance information required by the FLOSS License List or FRB;

v. includes any required Company notices;

vi. conforms to the Company's code of conduct and policies for FLOSS Contributions; and

vii. is consistent with the FLOSS 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 FLOSS 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 FLOSS 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.

1. General

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

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

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

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

a. Code of Conduct

b. Intellectual Property

c. Technology Acquisition

d. Social Media

e. Business Process Change Management

f. Information Security

g. Information Classification

h. Electronic Communications

i. Software Development & Maintenance

j. Software and IT Infrastructure Development Lifecycle

k. Source Control Management

l. Secure Coding

1. Definitions

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

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

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

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

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

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

F. FLOSS 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).

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

H. FLOSS Request: A FLOSS Use Report or FLOSS Contribution Request.

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

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

K. FLOSS Request System: An internal system for submitting, discussing, and resolving FLOSS Requests.

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

M. FLOSS Training Program: The training program described by Section 5 of this Policy.