Linux Foundation Compliance Program: Generic FOSS Policy

The Linux Foundation Open Compliance Program
http://compliance.linuxfoundation.org/

Introduction

On August 10, 2010, the Linux Foundation announced the availability of the Open Compliance Program (OCP). Led by experts in free and open source software (FOSS) compliance and backed by such organizations as Adobe, AMD, ARM Limited, Cisco Systems, Google, HP, IBM, Intel, NEC, Novell, Samsung, Software Freedom Law Center, Sony Electronics, to name a few, the OCP was established with some noteworthy goals in mind:

- to boost adoption of Linux and other FOSS by making license compliance ever-easier to achieve
- to increase awareness and understanding of FOSS compliance responsibilities
- to make available free resources that can help companies establish their FOSS compliance programs

Today, the Open Compliance Program offers:

1. Comprehensive and neutral training in implementing and managing compliance programs
2. Compliance educational materials (white papers, webinars)
3. Free tools to help companies be more efficient with their compliance due diligence
4. An online community (FOSSBazaar) dedicated to exchanging FOSS policies, processes and governance best practices
5. A checklist with over 100 FOSS compliance practices found in industry-leading compliance programs
6. A rapid alert directory of company compliance officers
7. SPDX™, a standard record of licensing and copyright information for all runtime dependent files contained in a software package (e.g., source files, libraries, programs).
8. Generic compliance related templates to help companies bootstrap their FOSS programs

Companies using FOSS often create a company-wide policy to ensure that all staff is informed of how to use FOSS (especially in products), to maximize the impact and benefit of using FOSS, and to ensure that any technical, legal or business risks resulting from that usage are properly mitigated.

This document is a new free resource available from the Linux Foundation under the Open Compliance Program. It offers a generic FOSS Policy that companies can use as starting point in creating their own FOSS Policy. It provides a template policy that focuses on governing FOSS usage in externally distributed products that can be customized to the company's specific needs.

Feedback and Future Revisions

Suggestions for improvement of this generic FOSS Policy will be appreciated. Please send comments to compliance@linuxfoundation.org. Feedback provided to the Linux Foundation is confidential to encourage organizations and individuals to freely share their thoughts.

<Company's> Free and Open Source Policy

Abstract: This document defines <company's> policy for the use of free and open source software in externally distributed products.

Document ID: <document ID>
Revision No.: <revision number>
Revision Date: <revision date>

Summary

Revision	Date	Author	Description of Change
<revision no.>	YYYY-MM-DD	<author>	
0.1	2012-05-23	First and Last Name	This is initial 0.1 draft of the policy.

All questions about this policy should be directed to OSRB@companyname.com.

Purpose

The policy defined in this document enables <company> to benefit from the use of free and open source software (FOSS) while ensuring compliance with FOSS license terms and values and respecting third party intellectual property rights.

This document provides a common framework for FOSS compliance for the entire organization, with the goal of ensuring license compliance. The policy will provide employees an understanding of how to work with FOSS, and will establish corporate intent to respect free and open source software and to contribute purposefully to open communities.

Scope

The policy and procedures described herein apply whenever employees, independent contractors, and/or vendors incorporate FOSS into <company> products that are or may be distributed externally. It is the responsibility of the manager retaining independent contractors to ensure the independent contractors are aware of, and follow, this policy. Use of FOSS for purely internal purposes is not constrained by this policy.

Policy and procedural steps also apply whenever a <company> employee contributes to a work-related FOSS project or whenever <company> contemplates contribution of code to a FOSS project. <company> will not require approval for employee contributions to non-work-related FOSS projects.

Terms and Abbreviations

Free and Open Source Software (FOSS) - shall mean any publicly available software that may be copied, modified and redistributed in source code format without charge, including, but not limited to, any publicly available software licensed under one of the licenses listed by the Open Source Initiative on its web site at: **http://www.opensource.org/licenses/**.

OSRB - Open Source Review Board

Policy

Procedures, work instructions, training, and tool support must be established to implement compliance processes for each of the following use cases (and any others in which software is conveyed externally by <company>).

Inclusion of FOSS in a <company> deliverable

The compliance process shall include (but not necessarily be limited to):

- Identification of all FOSS contained in the <company> deliverable
- Submission of a request to the OSRB to use identified FOSS packages
- Review (including architectural dependency analysis, provenance analysis for identified FOSS, license identification and analysis, analysis of potential impact to intellectual property rights, etc.)
- Approval decision
- Identification of obligations to be satisfied
- Satisfaction of obligations

Third party commercial software acquired for distribution by <company>

The policies in this document apply to packaged software licensed by vendors as well as contracted development of custom software. A developer that delivers software to <company> must disclose any FOSS contained in its deliverable, including

- A list of all FOSS components, including their version numbers
- All applicable licenses (not only the main license but each applicable license)
- Material for product documentation (including but not limited to license texts, copyright notices, acknowledgments and attributions)
- Source code for the FOSS (when applicable), including any modifications made by the developer
- Dependency charts illustrating the dependencies, interfaces, and interactions between the FOSS components and any other product components

All use of FOSS in software delivered to <company> must be reviewed and approved by <company>.

Specific rules for server software

If server software includes FOSS licensed under the Affero General Public License (AGPL) or similar license, such use must be reviewed and approved according to the process defined for FOSS included in a <company> deliverable. If server software is distributed to a third party for hosting or distributed to an external party for any other purpose, use of any FOSS must be reviewed and approved. Otherwise, use of FOSS in server software hosted by <company> need not be subjected to review and approval.

Contributions to FOSS projects

The policies in this document apply to both company contributions of source code and individual contributions of time and effort to FOSS community projects. For the purposes of this policy, “contribution” means making software and/or related material (descriptions, documentation) for which <company> holds the copyright available to third parties, or to the general public, under an open source license, granting access, modification and/or distribution rights with regard to the software in source code form.

<company> wishes to encourage contributions and community involvement in order to advance worthy technologies and projects; align a FOSS project with <company> technology roadmaps; provide bug fixes and feature enhancements to FOSS used by <company>; and minimize future maintenance costs, among other reasons.

The policy’s provisions seek to ensure that contributions align with <company> interests, contributions do not cause technology fragmentation, and contributions do not accidentally compromise <company> intellectual property rights. Review of planned contributions will also clarify copyright ownership and licensing.

Plans for contributions (both company and individual) shall be submitted for review and approval to the FOSS Steering Committee, according to procedures the Committee will develop with the assistance of the FOSS Program Office.

Roles and Responsibilities

The following roles and responsibilities will be performed to assure effective implementation of the compliance process.

FOSS Steering Committee

The FOSS Steering Committee establishes company strategy for FOSS use and for FOSS community involvement and contributions. The Steering Committee will establish a procedure for reviewing requests to contribute to specific FOSS projects and communities.

FOSS Compliance Officer

The FOSS Compliance Officer is chiefly responsible for assuring compliance of <company> products with FOSS obligations. The Compliance Officer chairs the OSRB, directs the activities of the FOSS Program Office, acts as liaison to product teams to assure compliance processes are understood and followed, and escalates issues to executive management, as needed. The Compliance Officer also replies to compliance inquiries from external entities and responds to questions concerning <company> use of FOSS.

FOSS Program Office

The FOSS Program office is the center of expertise in FOSS compliance and takes responsibility for process definition and deployment, including procedures, tools, forms, templates, work instructions, and other measures to achieve compliance effectively. Program Office staff take the lead in identifying modifications to existing company business practices to incorporate FOSS compliance considerations. The Program Office develops and delivers training in compliance practices, and leads compliance tool selection/development and deployment. Program Office staff also perform or monitor code audits and automated scans to identify FOSS inclusion in <company> products; maintain an inventory of <company> FOSS use and accurate records regarding OSRB decisions; conduct process adherence audits; independently verify product distribution readiness with respect to FOSS compliance; and develop and maintain a company web portal for FOSS access.

Open Source Review Board (OSRB)

The OSRB reviews and approves requests to use FOSS in company products, analyzing product designs and license obligations to assure appropriate use of FOSS. The OSRB interacts with product teams to obtain information needed for its analyses. It assures that license obligations are clearly understood by product teams and that obligations will be satisfied.

Product Team

The Product Team identifies FOSS to be used in its products and submits requests for approval to the OSRB in a timely manner, providing all requested information. The Product Team takes responsibility for satisfying obligations of applicable FOSS licenses for its products.

Supply Chain

The supply chain function assures that all third party suppliers of software for <company> products understand their FOSS compliance responsibilities, make timely disclosures of FOSS used in their deliverables to <company>, and provide any and all information and source code needed for <company> to meet its own obligations for FOSS contained in products it distributes.

Law Department

The Law Department interprets FOSS licenses and their obligations; provides guidance to product teams in satisfying those obligations; advises the OSRB on licensing and intellectual property issues, including conflicts arising from incompatible FOSS licenses; participates in OSRB deliberations and approval decisions; provides input to business teams and the FOSS Steering Committee on requests to contribute to community projects; and advises the FOSS Compliance Officer and FOSS Program Office in responding to external compliance inquiries.

Ombudsman

The ombudsman role provides an independent and confidential channel of communication for employees with concerns about <company> decision-making with respect to FOSS compliance issues.

Approval

This policy shall be effective immediately upon approval.

Title	Approver	Signature	Effective Date

========== END FOSS Policy Template ==========

Linux Foundation Compliance Resources

Compliance Training
The Linux Foundation offers hands-on training from compliance experts for individuals and companies responsible for achieving compliance with FOSS licenses and establishing a FOSS compliance program, as well as for those who simply want to learn more about compliance.

Self-Assessment Checklist
An extensive checklist of practices found in industry-leading compliance programs. Companies use this checklist as a confidential internal tool to assess their progress in implementing a rigorous compliance process and help them prioritize their process improvement efforts. To provide feedback on the checklist, email **compliance@linuxfoundation.org**.

Compliance Templates
When a company is in the process of creating a FOSS compliance program, they need to establish policy, processes, guidelines, best practices, and much more. The Open Compliance Program is offering some of these material as templates that you can customize to your own needs saving you the effort to start from scratch.

Compliance Publications
Over a dozen papers are available from **http://www.linuxfoundation.org/publications/compliance**.

Open Compliance Directory and Rapid Alert System
A directory of compliance officers at companies using FOSS in their commercial products to enable faster and direct communication between companies and FOSS developers around compliance.

Compliance Tools
Available from **http://www.linuxfoundation.org/programs/legal/compliance/tools**. To participate in the development of these tools, visit **http://git.linuxfoundation.org/** and **http://bugzilla.linuxfoundation.org/**.

The Software Package Data Exchange™
The SPDX™ specification is a standard format for communicating the components, licenses and copyrights associated with a software package.

FOSSBazaar
An open community of technology and industry leaders who are collaborating to accelerate adoption of FOSS in the enterprise.

About the Open Compliance Program
The Linux Foundation's Open Compliance Program is the industry's only neutral, comprehensive software compliance initiative. By marshaling the resources of its members and leaders in the compliance community, the Linux Foundation brings together the individuals, companies and legal entities needed to expand the use of FOSS while decreasing legal costs and FUD. The Open Compliance Program offers comprehensive training and informational materials, open source tools, an online community (FOSSBazaar), a best practices checklist, a rapid alert directory of company's compliance officers and a standard to help companies uniformly tag and report software used in their products. The Open Compliance Program is led by experts in the compliance industry and backed by such organizations as the Adobe, AMD, ARM Limited, Cisco Systems, Google, HP, IBM, Intel, NEC, Novell, Samsung, Software Freedom Law Center, Sony Electronics and many more. More information can be found at **http://www.linuxfoundation.org/programs/legal/compliance**.