OpenChain 规范

版本 2.1

本规范功能上等同与:

- **OpenChain 规范 2.0**
- **ISO/IEC PRF 5230**

更多信息: www.openchainproject.org

目录

前言

本文档定义高质量开源许可合规方案的关键要求。其目标为提供一个基准，在交换由开源软件组成的软件解决方案的组织之间建立信任。规范合规性确保了方案设计的目的是为每个软件解决方案生成所需的合规资料（例如法律声明，源代码等）。本规范聚焦于开源合规方案的“是什么”和“为什么”，而不是考虑“如何”和“何时”。这将确保实际操作的灵活性，使得不同的组织能够定制跟他们规模，目标和范围最符合的政策和流程。举例来说，OpenChain 合规方案可以涵盖单个产品线或整个组织。

前言为所有潜在用户提供了背景内容。第二章定义了贯穿本规范所使用的关键术语。第三章定义了实现合规方案必须要满足的要求。此要求包含一个或多个核查材料（例如记录）以确保能满足要求。核查材料并不需要公开，但是该组织可以根据保密协议（NDA）选择提供给其他人。

本文档作为开放性倡议已收到 200 多投稿人的反馈。通过查看规范邮件列表和常见问题解答(FAQs)，可以深入了解其历史发展。

信息技术 — OpenChain 规范

1 范围

本文档规定开源许可合规方案的关键要求，以提供在交换由开源代码软件组成的软件解决方案的组织之间建立信任的基准。

2 术语与定义

以下术语和定义适用于本文档。

2.1
合规资料

对一个交付软件进行开源合规管理的方案所输出的一组资料的集合。

注：资料集可能包括（但不限于）以下一项或多项：属性通知、源代码、构建与安装文稿、许可证副本、版权声明、修改通知、提供源代码的书面文件、开源组件材料清单和 SPDX 文档等。

2.2
已识别的许可证

一组经过适当方法来识别构成交付软件的开源组件的开源许可证。

2.3
OpenChain 合规性

满足本文档所有要求的方案。

2.4
开源软件

使用一个或多个许可证的软件，这些许可证符合开源代码方案发布的开源定义（请参见 opensource.org/osd)或者自由软件基金会发布的自由软件定义（参见 gnu.org/philosophy/free-sw.html) 或类似许可证。

2.5
方案

一套用于管理组织内开源合规行为的政策、流程和人员。

2.6
方案参与者

定义、参与或负责准备所提供软件的任何组织雇员或承包商。

注：有些组织可能包括（但不限于）软件开发人员、发布工程师、质量工程师、产品营销和产品管理。

2.7
SPDX

由 Linux 基金会旗下 SPDX（Software Package Data Exchange）工作组为交换给定软件包的许可证和版权信息而创建的格式标准。包括相关的许可证和版权信息（参见 spdx.org）

2.8
交付软件
组织向第三方（例如其他组织或个人）交付的软件。

2.9
核查材料
证明满足规范指定要求的材料。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

— ISO 在线浏览平台：可在 https://www.iso.org/obp

— IEC Electropedia 可在 http://www.electropedia.org/

3 要求

3.1 方案基础

3.1.1 政策

存在一份书面的开源软件政策，用于管理交付软件的开源合规性。该政策必须在内部传达。

核查材料：

- 3.1.1.1 存在一份有记录的开源政策文档
- 3.1.1.2 存在一个有记录的流程，用于让软件员工知晓该开源管理政策（例如培训、内部 Wiki 或者其他实际可行的内部沟通方式）。

理由：

确保采取步骤来制定和记录政策，并使得软件工作人员认识到该开源管理政策的存在。虽然此处没有对政策中包含的内容提出任何要求，但是其他章节可能会对内容提出要求。

3.1.2 能力

该组织应该

- 确定影响项目绩效和有效性的角色和相应的职责；
- 确定项目参与者履行每个角色所需的能力；
- 确保项目参与者在适当的教育、培训和/或经验基础上能够胜任；
- 如果可行，采取行动以获得必要的能力，或
- 保存适当的文档作为这些能力的证明。

核查材料：

- 3.1.2.1 一份有记录的文档，列举开源合规方案中不同参与者的角色和对应责任。
- 3.1.2.2 一份文档来明确各个角色的能力。
- 3.1.2.3 每个方案参与者能力评估的书面证明。

理由：

确保方案参与者具备足够的能力胜任各自的角色和职责。

3.1.3 知晓

组织应确保项目参与者了解：

- 开源政策；
- 相关开源目标；
- 参与者对于方案效率的贡献；以及
- 未能遵守方案要求的影响。

核查材料：

- 3.1.3.1 一份评估每个方案参与人员的意识的书面证明，包括方案目标，人员贡献以及未能遵守方案要求的影响。

理由：

确保方案参与人员对于本方案中各自角色和职责有足够的认识。

3.1.4 方案范围

不同的方案可能适用不同的范围。例如，一个方案可能管理一个产品线、整个部门或整个组织。每个方案都必须声明其方案适用的范围。

核查材料：

- 3.1.4.1 明确规定方案范围和限制的书面声明。

理由：

提供灵活的开源合规方案以最佳符合组织范围的要求。某些组织可以选择在某个特定产品线实行一个方案，而在整个组织内实行另一个方案来管理交付软件。

3.1.5 许可证义务

存在一个审查已识别的软件许可证的流程，以确定每个开源许可证所授权的义务，限制和权利。

核查材料：

- 3.1.5.1 存在一份有记录的流程，用来审查和记录每个已识别的开源许可证授予的义务，限制和权利。

理由：

确保存在一个审查已识别的许可证义务的流程，用于组织内各种应用场景（如§3.3.2 所定义）。

3.2 定义并支持相关任务

3.2.1 联络

维护有效响应外部开源查询的流程，公开确定第三方可以进行开源合规查询的方式。

核查材料：

- 3.2.1.1 具备公开可见的方式以允许任何第三方进行开源合规查询（例如通过一个公开的邮件地址，或 Linux 基金会的开源合规联系目录）。
- 3.2.1.2 一份内部有记录的流程来描述如何响应第三方开源合规查询。

理由:

确保组织具有一个合理的方式，能够联系和有效响应来自第三方的开源合规查询。

资源有效性

确认并为方案任务分配资源:

- 分配责任以确保方案任务的成功执行。
- 方案任务具备充分资源：
  - 已分配履行该任务的时间；并且
  - 已分配充足的资金。
- 存在一个用于审查和更新政策和支持任务的流程；
- 需要指导的人可与开源合规相关的法律专家进行接触；并且
- 存在一个解决开源合规争议的流程。

核查材料：

- 3.2.2.1 一份文档用来记录方案中确切人员，团体或职责的确切名称。
- 3.2.2.2 方案中角色的人员已有明确安排，并提供充足的资金。
- 3.2.2.3 确认有内部或外部的法律专家用来解决开源合规事宜。
- 3.2.2.4 一份流程文件来描述如何分配内部开源合规的职责。
- 3.2.2.5 一份流程文件来描述如何审核和修复不合规事项。

理由：

确保：i) 方案责任得到有效的支持和充分资源以及 ii) 定期更新政策和支持流程，以适应开源合规最佳实践的变化。

3.3 审查及批准开源内容

3.3.1 材料清单

存在一个流程用于建立和管理材料清单，该清单包含组成交付软件的每个开源组件（和它已识别的开源许可证）

核查材料：

- 3.3.1.1 一份有记录的流程，用于识别、跟踪、审查、批准和归档组成该交付软件的开源组件集合。

- 3.3.1.2 每个交付软件都需具备开源组件记录，以证明该流程被正确的执行。

理由：

确保存在一个流程，用于创建和管理该软件包含的开源组件清单。该清单用于支持对每个开源组件的许可证条款进行系统审查和批准，以了解适用于所提供软件分发的义务和限制内容。

3.3.2 许可证合规

此方案必须能够管理软件工作人员在处理所提供软件时经常碰到的开源许可证使用案例，其中可能包括下列使用案例（注意本列表并未详尽，也可能不适用于所有的使用案例）：

- 以二进制方式发布；
- 以源代码方式发布；
- 与其他开源项目集成，可能会触发附加许可义务；
- 包含修改过的开源软件源代码；
- 包含开源软件或者其他软件，使用与交付软件中的组件不兼容的许可证；
- 包含带有权属要求的开源软件源代码。

核查材料：

- 3.3.2.1 存在一个有记录的流程来处理在交付软件的开源组件中常见的开源许可证案例。

理由：

确保方案足够强大，可以处理组织常见的开源许可证案例。存在支持此活动的流程并被遵守。

3.4 创建并交付合规资料

3.4.1 合规资料

存在为交付软件创建一套合规资料的流程。

核查材料：

- 3.4.1.1 一份有记录的流程，确保按照已识别的许可证的要求进行准备和分发的合规性材料随该软件一并分发。
- 3.4.1.2 一份有记录的流程，该流程是为了将交付软件的合规资料副本进行归档，而归档的副本，须自交付软件最后一次提交时起，保存一段合理时间[1]，或依已识别的许可证的要求进行保存(以时间较长者为准)。此外，须留存相关记录，以证明已正确遵循该流程。

理由：

为了确保按照已识别的许可证的要求，在准备交付软件所附的合规资料时作出了合理的商业努力。

[1] 由域、司法管辖权和/或客户合同所决定

3.5 理解开源社区的参与

3.5.1 贡献

如果一个组织允许对开源项目进行贡献，则

- 存在一份书面的政策来管理对开源项目的贡献；
- 该政策须在该组织内部传达；以及
- 存在一个流程以实施该政策。

核查材料:

如果一个组织允许对开源项目进行贡献，则须具备：

- 3.5.1.1 一份有记录的开源贡献政策；
- 3.5.1.2 一份有记录的开源贡献管理流程；以及
- 3.5.1.3 一份有记录的流程(如：培训、内部 Wiki 或其他可行的传达方式)，以确保所有软件工作人员知晓该开源贡献政策的存在。

理由：

当一个组织允许开源贡献时，我们希望确保该组织已充分考虑，来制定并实施一份贡献政策。开源贡献政策可以是整体开源政策的一部分，也可以是一个独立的政策。

3.6 遵守规范的要求

3.6.1 合规性

为了使方案被视为满足 OpenChain 合规性，该组织必须确认该方案满足本规范中提出的要求。

核查材料:

- 3.6.1.1 一份正式声明文件，确认规范§**Error! Reference source not found.**中规定的方案符合本规范的所有要求。

理由：

为确保当一个组织声明其方案是遵守 OpenChain 规范时，该方案已符合本规范的所有要求。仅符合本规范的一部分要求是不够的。

3.6.2 持续期间

符合此版本规范要求的合规方案将从获得 OpenChain 合规性认证之日起持续 18 个月。合规性认证注册方案请见 OpenChain 项目的网站。

核查材料:

- 3.6.2.1 在获得合规性认证的 18 个月内，存在一份文档来确认本方案符合本规范的所有要求。

理由：

如果一个组织希望声明其方案是持续遵守本规范的，则须与本规范的最新版本保持同步。此要求确保该方案的支持流程与管理不会随着时间流逝而弱化。

附录 A
(有用信息)

本规范的其他语言版本

为了促进全球采用，我们欢迎将本规范翻译成不同语言。由于 OpenChain 是一个开源项目，因此相关的翻译工作，皆是由愿意贡献时间与专业知识的贡献者，依照 CC-BY-4.0 许可证以及本项目的翻译政策来推动的。该翻译政策的细节与现有的翻译版本，请见 OpenChain 项目规范的网页。