OpenLogic

Open Source Policy Builder

The following questions represent components of a comprehensive open source policy. Each question has several policy choices listed below. Your organization can build its open source policy by answering the questions and formulating language expressing its choices in a policy statement. Examples of how policy choices can be expressed as policy statements are given in Question 1.

1. Which licenses are approved for use by the company?

Choices

- All Open Source licenses
- OSI-approved licenses
- All except reciprocal licenses
- Company-specified list:

Example Policy Statement

All: 'Software distributed under all Open Source licenses is permissible [link to review process].'

OSI-approved: 'All OSI-approved licenses are approved [specify exception process]'

Company-specified list: 'The following licenses are approved for use [approved list] [specify exception process]'

2. External Acquisition – where can an end-user obtain source code? Where can you acquire the "canonical source"?

- From the Internet, any source (SourceForge, FreshMeat, Krugle, Google, OSDir, other repositories)
- Directly from the community source or record
- From a third party supplier, i.e. Red Hat, IBM, Covalent

3. Internal Acquisition – how is the 'canonical' source distributed internally?

- Anybody can obtain the source
- There must be a centralized location internally, e.g. a server where people can download internally
- There is a manual process

4. **Who/what level in the organization is responsible for understanding and ensuring compliance with the terms and conditions of OSS licenses?**
   - Legal
   - Audit
   - Engineering Managers
   - Individual Developers
   - IT management
   - Central OS Review Board
   - Other
   - All of the above

5. **Business Justification**
   - None needed
   - Must meet engineering requirements
   - Must demonstrate business value – TCO vs functionally-equivalent commercial software, ROI, etc.
   - Need to demonstrate why OSS was chosen over a commercial solution

6. **Who is the owner? Who is responsible for initial acquisition and lifecycle management of an OSS component?**
   - Individual end-user
   - Each OSS component has a 'named' owner (can be used in 20 divisions)
   - One person or central body/team, e.g. OSS Review Board

7. **How is acquisition initiated?**
   - Acquisition is the responsibility of the individual developer
   - Acquisition is the responsibility of the Procurement/Supply Chain Management
   - Acquisition requests are directed to the central body/team

8. **Security and Integrity: What kind of security/integrity review must OSS undergo before it is procured?**
   - None
   - Download from trusted source is sufficient
   - MD5 Checksum or other prevailing security verification method
   - Virus scan with an up-to-date fingerprint library
   - Complete source code scanning for security and integrity
   - Manual review

9. **Warranty: What warranties must be obtained from OSS vendors? (e.g. free replacement of IP infringing code)**
   - None, terms of OSS license is sufficient (no warranties)
   - Warranty scales with risk – if internal infrastructure use, none needed – if customer-facing, warranty required [criteria needed – EXERCISE]
   - All OSS must be obtained from a source that provides warranty

10. **Indemnification: What kind of indemnification must be obtained from OSS vendors?**
    - None; terms of license sufficient
    - Scales with risk [criteria needed - EXERCISE]
    - Full indemnification

11. **Policy Scope: What is the scope of the OSS Policy?**
    - Enterprise-wide
    - Divisional/LOB
    - Department

12. **Remediation: Once this policy is established, what are remediation requirements with respect to existing OSS?**
    - None, grandfathered in
    - Existing OSS inventory must be inventoried within X days
    - All existing OSS inventory must be immediately remediated per policy

13. **OSS Architecture: Is there a minimum technical standard that OSS must meet to be considered for acquisition?**
    - Minimum: None – developers take all the responsibility, use at own risk
    - Project is considered stable in SourceForge/Freshmeat and/or community must be considered stable
    - Must have significant widespread adoption as measured by downloads
    - Must have significant commercial base, i.e. MySQL dual-license

14. **Forking/Community Abandonment: How will the company deal with project forking or abandonment? Are there alternate vendors/suppliers available?**
    - Will deal with it when it happens
    - Must have alternate vendor/suppliers listed or identified
    - Must have active written response plan
    - Must test and deploy backup
    - Must have deploy dual-standard, must have two-vendor integrity, must have backup source available at all times (e.g. Hibernate and BEA Topspin)

15. **Certification: Do OSS components have to be certified before they can be implemented or deployed? If so, who must certify and what kinds of certification must be done? When can OSS be deployed to production?**
    - None, no certification needed
    - Locally certified by ‘owner’ or end-user
    - Formal certification by central IT staff
    - External certification, e.g. BRR
    - Commercial certification, e.g. IBM, HP, OpenLogic

16. **Will OSS be distributed ?**
    - No, all use is internal
    - No, but will be used in customer-facing environments
    - Yes, will distribute unmodified OSS externally
    - Yes, will distribute modified OSS externally
    - Yes, will integrate and distribute OSS with proprietary IP

17. **Can OSS be modified?**
    - No, must be used in native form
    - Can be modified with approval [EXERCISE: what is approval]
    - Can be modified in specified ways [EXERCISE: what are specified modifications?]
    - Can be modified in any way if not distributed
    - Can be modified without restriction

18. **Who is responsible for maintaining inventory, usage and other metadata related to OSS component, including licenses?**
    - Individual end-user
    - Each OSS component has a ‘named’ owner (can be used in 20 divisions)
    - One central person or central body/team, e.g. OSS Review Board

19. **Security: Who will be responsible for overseeing security of OSS components? Who will check if the code contains vulnerabilities? Who is responsible for applying security patches?**
    - Individual end-user
    - One central person or central body/team, e.g. OSS Review Board
    - Team to be named
    - IT Security staff

20. **Will contributions be allowed?**
    - No
    - Yes, by indirectly via use of a proxy
    - Yes, with valid business need and/or approval from management
    - Yes, unregulated

21. **Under what circumstance can an employee make a contribution to an OSS project if it is not related to company business?**
    - Under no circumstance – possible violation of employment contracts
    - Yes, without attribution to company name and on employee's personal time

22. **Email communication: Under what circumstances can employees communicate with OSS communities (with company attribution)?**
    - Directly linked to contribution question (Q 20-21)
    - Never
    - When business need dictates
    - Freely for any reason

23. **Public Speaking**
    - No (e.g. Barclay's, Wells Fargo)
    - Yes, with prior management approval
    - Yes, with specified approved topics (e.g. Fidelity)
    - Yes, under any circumstance (e.g. Google)

24. **Support: What level of support must be in place prior to implementation**
    - Individual end-user responsibility
    - Provided by formal internal team, end-user or central IT
    - Combination internal with external provider
    - Must have SLA signed with business partner

25. **Where should OSS be housed?**
    - End-user responsibility
    - Centrally-managed repository
    - Vendor-managed repository (OpenLogic)

26. **Will source code scanning be required (for IP infringements)?**
    - No
    - Yes, source code must be fingerprinted upon initial acquisition only
    - Yes, source code must be scanned periodically
    - Custom list

27. Project Tracking: how is OSS tracked?

- No special project tracking
- Yes, in custom-built project tracking tool
- Yes, with vendor-provided tool (e.g. OpenLogic, Black Duck, etc.)

28. Offshoring/Outsourcing/Contracting

- None, responsibility of contractor to make sure they are adhering to OSS licenses
- Must make sure things are complementary – contractor policy should sufficiently be comparable in scope to Company's, or vendor must commit to follow Company's policy
- All engagements must adhere to every part of company's OSS policy