Open-Source Software (OSS) Policy

Version 1.0
Effective Date: [Insert Date]
Approved By: [Executive Sponsor or Board]

1. Purpose

This policy establishes how [Company Name] adopts, manages, and contributes to open-source software (OSS). While OSS enables innovation, rapid development, and cost efficiency, unmanaged use introduces risks in licensing, intellectual property, security, and long-term support. The goal of this policy is to maximize OSS benefits while ensuring compliance with all legal and business requirements.

2. Scope

This policy applies to:

- All employees, contractors, and third parties working on software for [Company Name].
- All OSS components included in products, services, internal tools, prototypes, or proof-of-concepts.
- Contributions to external OSS projects when made on behalf of the company.

3. Guiding Principles

- **Encourage Responsible OSS Use** – OSS should be leveraged where it accelerates development and adds value.
- **Maintain Compliance** – All OSS use must adhere to license obligations and company IP strategy.
- **Prioritize Security** – OSS components must be actively maintained, patched, and monitored for vulnerabilities.
- **Transparency** – All OSS usage must be documented in a centralized inventory (SBOM).

4. Requirements

4.1 Approval & Intake Process

- Developers must submit proposed OSS components for review before inclusion.
- Reviews assess:
    - **License obligations** (MIT, Apache 2.0, GPL, AGPL, etc.)
    - **Security posture** (CVEs, update frequency)
    - **Community health** (number of maintainers, activity on GitHub, last commit date)
- Restricted licenses (e.g., GPL, AGPL, SSPL) require **legal sign-off**.

Example: Using an MIT-licensed JSON library → Low risk, quick approval.
Using GPL-licensed encryption library → Requires legal approval and business justification.

4.2 License Compliance

- Attribution and copyright notices must be included in the product's "About" page, documentation, or license file.
- Source code disclosure obligations (e.g., GPL) must be fulfilled if triggered.
- Employees may not circumvent license requirements by modifying or re-packaging OSS.

4.3 Security & Maintenance

- All OSS components must be scanned in CI/CD pipelines with an **SCA tool** (e.g., Snyk, Sonatype, Aqua).
- Critical vulnerabilities (CVSS 9.0+) must be remediated prior to release.
- Medium vulnerabilities must be patched in the next scheduled sprint.
- Dependencies must be updated at least quarterly, even if no vulnerabilities are present, to ensure currency.
- End-of-life or unmaintained components must be replaced.

4.4 Contributions to OSS

- **Personal Contributions:** Employees may contribute to OSS on personal time provided it does not conflict with company IP or confidentiality obligations.
- **Company Contributions:** Contributions on behalf of [Company Name] require approval from Engineering Management and Legal. A Contributor License Agreement (CLA) must be reviewed where applicable.

5. Documentation & Inventory (SBOM)

- A **Software Bill of Materials (SBOM)** shall be maintained for all products.
- Inventory entries must include:
    - Component name and version
    - License type
    - Approval status
    - Known vulnerabilities (if any)
    - Date of last review
- The SBOM must be updated for every release and made available for customer requests and audits.

6. Roles & Responsibilities

- **Engineering Teams** – Identify, request, and document OSS components.
- **Security Team** – Conduct vulnerability scanning and monitor advisories (e.g., NVD, GitHub Security Advisories).
- **Legal/Compliance** – Evaluate licenses, approve/reject restricted components, and maintain compliance guidance.
- **OSS Review Board** (optional for larger orgs) – Multi-disciplinary team overseeing OSS governance.

7. Enforcement & Review

- Non-compliance may result in removal of components, product delays, or disciplinary action.
- This policy will be reviewed annually by Legal, Security, and Engineering leadership to ensure alignment with evolving OSS practices and laws.