Annex A. STF Contribution Policy

Programs and Projects Governance

This document describes the Software Transparency Foundation's Contribution Policy. It complements the STF Programs and Projects Governance Document, as Annex A .

- Name: Software Transparency Foundation Contribution Policy

- Reference: Annex A

- Responsible:

  - Approval: STF Governing Board

  - Management/maintenance: STF Programs Steering Committee

- Approval date: under review

1. – DEFINITIONS

- **IP**: refers to Intellectual Property
- **CLA**: Contribution License Agreement
- **iCLA**: Individual Contribution License Agreement
- **oCLA**: Organization Contribution License Agreement

2. – POLICY DESCRIPTION

STF Projects welcome contributions from individuals and organizations who agree to follow STF's values and governance.

The STF Contribution Policy establishes the framework for accepting contributions to all STF Programs and Projects. This policy applies to all forms of contributions including source code, documentation, data sets, services, designs and other materials. Contributions must be made under clear, verifiable terms that ensure legal certainty, transparency, and compatibility with STF IP Policy and the others. ensuring legal clarity, intellectual property compliance, and alignment with the Foundation's open collaboration principles.

The STF Contribution Policy is approved by STF Governing Board, being the Programs Steering Committee the governing body in charge of developing, updating, maintaining it, communicating it and monitoring compliance with it.

3. – CONTRIBUTIONS SCOPE AND REQUIREMENTS

3.1. – SCOPE OF CONTRIBUTIONS

STF accepts various types of contributions across its domains, like:
- Open Source Software Program: source code, build scripts, configuration files, software documentation, test cases, bug reports, feature requests, and architectural designs.
- Open Data Program: data sets, data schemas, validation scripts, data documentation, metadata definitions, data collection methodologies, and data quality assessments.
- Service Program: service configurations, operational procedures, monitoring reports, deployment documentation, service interfaces, openAPIs definitions and implementations, and operational run books.
- Cross-Program: General documentation, governance materials, policy documents, community resources, educational content, and integration specifications.

Other contributions might be welcome too, after an evaluation.

3.2. – CONTRIBUTION REQUIREMENTS

3.2.1. – General Contribution Requirements

No contribution shall be accepted into any STF Project unless and until the contributor has satisfied all of the following conditions:

- Acknowledgment of Governing Documents: the contributor shall acknowledge and agree to be bound by the STF Charter.
- Acceptance of the STF Code of Conduct: the contributor shall accept and agree to adhere to the STF Code of Conduct.
- Compliance with IP and Licencing policies: the contributor shall comply with all applicable STF Intellectual Property and Licensing Compliance Policies.
- Submission of a valid Contributor License Agreement (CLA), depending on their contributor status:
  - Individual CLA (iCLA): required for natural persons, contributing in their personal capacity.
  - Organization CLA (oCLA): required for individuals contributing in the course of their employment or engagement, or otherwise on behalf of a legal entity.

Each CLA shall grant to the STF Foundation the necessary rights to use, reproduce, modify, display, perform, sublicense, and distribute the contribution, in whole or in part, for any purpose, while preserving the contributor's ownership of the original work.

3.2.2. – Licensing requirements

All contributions must be compatible with the applicable outbound license of the receiving project. Inbound contributions must not introduce license conflicts or additional obligations. Software Transparency Foundation must publish and maintain a list of accepted licenses and usage guidelines for contributors for each Project.

All the details regardin license requirements are described in the Licensing Compliance Policy, an annex of the STF Programs and Projects Governance Document.

3.2.3.- Third-Party Dependencies

Contributors must clearly identify and document any third-party dependencies, ensuring:

- License compatibility with project requirements
- Compliance with STF Intellectual Property and other policies
- Proper attribution and license documentation
- Security assessment of dependencies

3.2.4.- Export Control Compliance

Contributors must ensure contributions comply with applicable export control regulations and the STF Export Control Policy, an annex of the STF Programs and Projects Governance Document.

Contributors must notify STF of any potential export control implications.

3.2.5.- Sensitive Data Handling

For contributions to Projects belonging to the Open Data Program, special procedures apply for:

- Personal data protection and anonymization requirements
- Compliance with applicable privacy regulations (GDPR, etc.)
- Data source authorization and licensing verification
- Ethical data collection and usage guidelines

All these procedures are explained in, among other STF policies, the STF Regulatory Compliance Policy, the STF Data Protection Policy, and the STF Contribution Policy

3.2.6.- Service Contributions framework

For service contributions, belonging to the Service Program, special procedures apply for:

- Formal service agreements defining scope, duration, and responsibilities

- Clear service level commitments and performance metrics

- Compliance with STF governance and operational policies

- Regular reporting and accountability mechanisms

- Defined termination and transition procedures

- Financial budgeting and reporting

4. – CONTRIBUTION LICENSE AGREEMENTS (CLAs)

All contributors must read, sign and submit the appropriate Contributor License Agreement before their contributions can be accepted into any STF Project. STF maintains two types of CLAs:

- Individual Contributor License Agreement (iCLA)
- Organization Contributor License Agreement (oCLA)

4.1. – INDIVIDUAL CONTRIBUTION LICENSE AGREEMENT (iCLA)

Required for individuals contributing on their own behalf, the iCLA:

- Grants STF perpetual, worldwide, non-exclusive rights to use, reproduce, modify, and distribute contributions
- Allows contributors to retain copyright ownership of their work
- Includes representations that:
  - The contributor has the right to make the contribution

- The contribution is original and the contributor is the author
- Covers patent rights necessary to use the contribution
- Requires disclosure of any known third-party intellectual property claims

4.2.– ORGANIZATION CONTRIBUTION LICENSE AGREEMENT (oCLA)

Required when contributions are made by employees or contractors on behalf of an organization, the oCLA:

- Establishes the organization's authority to make contributions and grant necessary rights
- Requires designation of authorized signatories who can execute iCLAs for employees
- Includes provisions for managing employee contributors and contractor relationships
- Addresses work-for-hire and intellectual property assignment policies
- Requires maintenance of current employee contributor lists

5.– CONTRIBUTION PROCESS

Contributions go through a structured process before the corresponding assets become part of STF. The process have four stages:

1. Submission: contributions are submitted via the official project infrastructure.
2. Review: contributions are reviewed by contributors and/or project Maintainers for technical quality, compliance with policies, and legal clarity.
3. Approval: the contribution is approved by Maintainers. Approved contributions are merged or accepted, with rationale documented in public STF channels.
4. Acknowledgment: contributors are credited and may be invited to participate further based on merit.

STF may introduce tools to automate CLA verification and to simplify the contributor onboarding process. All submitted CLAs and contributor records will be maintained securely by the STF for audit and compliance purposes.

5.1. – SUBMISSION STAGE

The Submission stage include the following requirements and actions, executed in the designated system by STF:

- Pre-submission
  - Account Setup: contributors must establish accounts on STF-approved platforms and communication channels so they can submit the contribution, track the evolution of the contribution process and respond to inquiries or questions
  - CLA Submission: Contributors must download, fill, sign and submit the appropriate CLA
  - Code of Conduct Acceptance: contributors must acknowledge and agree to follow the STF Code of Conduct
- Submission:
  - Proposal Discussion: for significant contributions, contributors should discuss proposals through appropriate project channels before implementation
  - Technical Implementation: contributors develop their contributions following project-specific guidelines and coding standards
  - Submission: contributions are submitted through established project workflows (e.g., pull requests, data submissions, service proposals)

5.2. – REVIEW STAGE

The Review stage includes the following requirements and actions, executed in the designated system by STF:

- Automated Checks: Contributions undergo software composition analysis, quality and security scanning, automated testing, format validation or any other checks for STF to understand the nature, evaluate the risks and the value of the contributed assets
- Technical Review. Project Maintainers review contributions for:
  - Technical quality and compliance with project, Program and STF standards
  - Security and data protection implications as well as best practices
  - Alignment with project roadmap and architecture
  - Documentation completeness and accuracy
  - Any other technical evaluation required to understand the technical nature, evaluate the technical risks and the technical merit of the contributed assets
- IP Clearance. Contributions are reviewed for:
  - License compatibility with project, program and STF requirements
  - Third-party dependency compliance
  - Patent implications and freedom to operate
  - Compliance with export control regulations
- Community Review. Contributions follow a community review process including:
  - Public discussion periods for significant changes
  - Consensus-building among stakeholders
  - Feedback incorporation and iteration

The workflow, orchestration and implementation of these actions and requirements might vary on the target Program and/or Project.

5.3. – APPROVAL STAGE

The Approval stage includes these actions and requirements:
- Final Approval: Maintainers provide final approval based on technical merit and Maintainers consensus. Contributors are notified of this approval.
- Integration: approved contributions are merged into project repositories or integrated into services.

5.4. – ACKNOWLEDGMENT

The Acknowledgment stage includes these actions and requirements:

- Attribution: Contributors are acknowledged in project documentation, release notes, contributor lists and in any additional channel, tool, collateral or material designated by the Project.
- Notification: Contributors and relevant community members are notified of successful integration

6. – RIGHTS AND RESPONSIBILITIES

The following rights and responsibilities rely on the Contributors and on STF:

- Contributor Rights. Contributors...
    - retain copyright ownership of their original contributions
    - may use their contributions in other projects subject to applicable licenses
    - receive public acknowledgment for accepted contributions
    - may participate in project governance according to established meritocracy principles
- Contributor Responsibilities. Contributors...
    - ensure legal authority to make contributions and grant required rights
    - verify that contributions do not infringe third-party intellectual property rights
    - follow project-specific contribution guidelines and coding standards
    - respond promptly to review feedback and address identified issues
    - maintain confidentiality of any sensitive information encountered during contribution process
- Software Transparency Foundation Rights and Responsibilities. STF...
    - receives necessary rights to use, publish, modify, and distribute contributions under project licenses

- commits to using contributions only in accordance with stated project licenses and Foundation principles
- will provide fair consideration of all contributions based on technical merit
- STF will maintain appropriate records of contributions and contributor agreements

7. – SPECIAL CONTRIBUTIONS

In addition to regular contributions, the Software Transparency Foundation (STF) welcomes special contributions, including one-time donations of assets such as datasets or curated archives, operational services and platforms, existing software projects or codebases, documentations and educational materials, intellectual property rights, infrastructure and hardware resources, and other digital or physical resources that can benefit STF Programs or Projects. Special contributions differ from standard contributions in terms of their origin, size, nature, or strategic relevance, and may involve pre-existing works or substantial resource transfers.

In addition to the corresponding requirements established by this policy, the Programs Steering Committee, guided by the STF Governing Board, might define a specific contribution process, including additional requirements, adapted to the nature and usage of the asset. Some of these requirements can be related with the effort needed to review and accept those assets as contributions.

Depending on the nature of the accept and complexity of the review and acceptance process, the Programs Steering Committee might adapt the Contribution Process timeline.

END