



AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

1 Executive Summary

This Policy is intended to provide the rules on the use of Free and Open Source Software (FOSS), Freeware, and Shareware at AT&T while mitigating the risks often associated with the use of this type of software by AT&T. Free and Open Source Software is often referred to simply as Open Source.

2 Contents

- 1 Executive Summary 1
- 2 Contents 1
- 3 Scope 1
- 4 Rationale 2
- 5 Employee Responsibility 2
- 7 Policy 4
 - 7.1 Software Development 4
 - 7.2 Use of Generative Artificial Intelligence (AI) for Code Development 4
 - 7.3 Inbound FOSS 5
 - 7.4 General Outbound Code Contribution Rules 6
 - 7.5 Outbound FOSS to Open Source Repositories (Contribution Types) 7
 - 7.6 External Distribution of AT&T Applications and Code 8
 - 7.7 Vendor-provided Open Source Software 8
 - 7.8 Foss Resources 9
 - 7.9 Employee Education and Compliance Obligations 9
- 8.0 Governance 9
- 9.0 FOSS Policy Exceptions 9
- Approvals 10

3 Scope

The Chief Information Officer and the Chief Security Officer maintain and govern this Policy. The Technology Strategies and Standards organization maintains this Free and Open Source Software (FOSS) Policy and is responsible for overseeing and managing the processes that govern it. This Policy provides important guidance for AT&T's use of FOSS in its operations. It is important that all employees using or contributing FOSS familiarize themselves with this Policy. This Policy applies to:



AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

- All AT&T employees and contractors.
- All FOSS licensed or otherwise brought into AT&T.
- Any development of FOSS by AT&T.
- Any development of software by AT&T using Generative or other AI technologies, including for example ChatGPT-like large language models (LLMs) or “Ask AT&T.”

This Policy supersedes and replaces any previous Policy on using FOSS, including Version 1.6 (2019) and Version 1.7 (2023). AT&T may amend or change this Policy periodically. Individual business units may not modify or otherwise revise this Policy. Any exceptions to this Policy must be requested in advance as set forth in Section 9 below.

This policy is in addition to AT&T Security Policy and Requirements (ASPR), and ASPR must also be reviewed for applicable security requirements.

4 Rationale

The acquisition, deployment, and use of FOSS can result in unreasonable risks to AT&T, including legal and financial liabilities that can negatively impact AT&T’s proprietary code, data, and information. The primary function of this Policy is maximizing the benefits of using FOSS within AT&T while reducing those risks.

This Policy helps ensure consideration is given to the legal, security, SME support, and asset management factors associated with the use of FOSS within AT&T.

5 Employee Responsibility

Compliance with this Policy is the responsibility of every AT&T employee or contractor that develops or uses FOSS products in software development. Failure to comply with this Policy may subject an employee to disciplinary action, up to and including dismissal. Employees with supervisory duties are responsible for ensuring all their subordinates know, understand, and comply with this Policy.

Any FOSS used at AT&T must be: (i) a standard offering at the AT&T Software Store or another AT&T repository of the TSS Now (Technology Strategies and Standards) organization, or (ii) software approved through the TSS Now process (See Section 7.3), or via an approved vendor to AT&T.

6 Definitions

Some terms found within this document are defined below.

Term	Definition
Free and Open Source Software (FOSS)	Any software with <i>source code</i> made available publicly for use, modification, distribution, or sharing. Subject to this Policy, such software code may be incorporated into or combined with other code used by AT&T, either within AT&T or externally as part of an AT&T product or service offering or other External Distribution. Such FOSS software or FOSS snippets also includes the output by a Generative AI tool.



AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

Generative AI	Any artificial intelligence or machine learning tool, such as ChatGPT or Ask AT&T, which can create software code without being explicitly programmed to do so. This is achieved using neural networks or deep learning algorithms that are trained on large datasets of existing software, allowing the tool to learn patterns and generate new software in response to user prompts. <i>Source: Ask AT&T</i>
Inbound FOSS	FOSS obtained by AT&T employees or contractors from the outside, e.g., GitHub, Stack Overflow, or Generative AI.
Outbound FOSS	FOSS that AT&T is contributing to an open-source community, repository, or other project under an AT&T-approved Open-Source License. This FOSS may be code that an AT&T employee or contractor developed or originated, including for example, Inbound FOSS which AT&T has modified or improved. Outbound FOSS should not be confused with External Distribution which is described below.
Open Source License	A type of software license allowing software source code to be used, modified, distributed, and/or shared under defined rules, terms, and conditions.
Copyleft License	A type of open-source license that requires AT&T to make its code publicly available. Specifically, if AT&T modifies copyleft code or combines it with AT&T proprietary code for external distribution, even as binary code, AT&T must make the entire AT&T code publicly available (i.e., the modified or the combined AT&T proprietary source code cannot be kept secret). Examples of Copyleft licenses are the GNU GPL family of licenses, the Eclipse Public License, and the Mozilla Public License).
Permissive License	An Open Source License that allows use and modification of source code without restrictions but is not a Copyleft License, i.e., because it grants rights to use FOSS without forcing users to license their source code modifications under the same license terms. Examples of Permissive Licenses are the MIT License, BSD 3-clause license, and the Apache License.
TSS Now Process	A request for approval to pursue a valid business use of FOSS but which is not approved under this FOSS Policy. Bringing FOSS into AT&T for production use when it is not available in an AT&T Repository or an AT&T vendor-approved repository. Such requests are made through TSS Now (sharepoint.com) . (See Sections 7.3 and 7.6 below).
External Distribution	External Distribution is dissemination or conveyance outside of AT&T of software, which includes FOSS, or otherwise exposes FOSS outside of AT&T's security system), for example as part of AT&T's product or service offerings. External Distribution includes anything that allows the FOSS (alone or as part of larger software) to be accessed or used outside of AT&T by its customers or others outside of AT&T. Examples of External Distribution include placement of the FOSS (i) in an AT&T app via a public app store; or (ii) on a home gateway or router; (iii) in AT&T's software for use by AT&T customers via a hosted environment (SaaS), or (iv) AT&T Website.

AT&T Technology Policy**Freeware, Shareware, and Open Source Software (FOSS) Policy**

7 Policy**7.1 Software Development****7.1.1 Scanning Software Applications:**

Software applications should be scanned for any FOSS used in the AT&T application at any time prior to production mode for license and plagiarism checks. The scan must be performed using an internal AT&T-approved scanning tool. The scanning tool must be capable of identifying not only whole FOSS modules within the AT&T software application, but also mere snippets of FOSS or other unidentified code contained within the software application. All software that is *externally distributed* must be scanned including at the snippet level. (See Section 7.6 for further guidance).

7.1.2 External Distributions

All External Distribution software must be approved by the Legal Department without exception. Such approval may be granted only upon providing the EULA, SBOM, Artifacts, Scan results, Distribution Mode, and applicable FOSS licenses associated with the FOSS in the software.

7.1.3 Use for Internal Operations or External Distribution:

Applications and software developed that contain FOSS must identify whether such software is intended for internal use by employees, contractors, or contracted business partners or whether it will be Externally Distributed.

7.1.4 Copyleft Licensed Code and Unidentified Code

Applications or software for External Distribution cannot contain or include FOSS, which is licensed under a Copyleft License, or for code which AT&T cannot determine the applicable licensing terms. Applications that are only used for internal operations may contain FOSS under a Copyleft License subject to the requirements of this Policy.

7.1.5 ASPR and Security Risks

Application Developers should work to identify and mitigate any security issues in accordance with ASPR requirements.

7.2 Use of Generative Artificial Intelligence (AI) for Code Development

Subject to Section 7.1, you may use AT&T approved Generative AI tools for AT&T employees to create software for AT&T operations with the following conditions:

7.2.2 BU Manager Permission:

You must obtain permission from your BU manager to create code using the approved AT&T Generative AI tool. Please document such permission from a Level 3 manager via email for your records.

AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

7.2.3 External Distribution of Generative AI Code:

You may NOT Externally Distribute code created using Generative AI without getting specific, approval via the TSS Now process, (including Legal approval). Only one request is necessary for each application you are distributing. You must identify in the TSS Now process request that the code was created using a Generative AI tool.

7.2.4 Copyleft Code or Unidentified Code:

You may not use Generative AI code for External Distribution if any snippet of the code is identified through scanning to be code licensed under a Copyleft License, or code for which AT&T cannot identify the applicable licensing terms. Any such copyleft-licensed or unidentified code must be removed from the Generative AI code.

7.2.5 Scanning Generative AI Code:

For Generative AI code, you must ensure that the code has been scanned using approved AT&T scanning tools for security vulnerability, identify third-party code snippets which may come from FOSS modules at GitHub, other repositories, Stack Overflow, or the web.

7.2.6 Required Documentation:

You must create the following: SBOM, including FOSS snippets, license identification contained in the Generative AI code created.

7.3 Inbound FOSS

The use of FOSS is acceptable and encouraged provided all established safeguards and procedures of this Policy are met.

7.3.1 Inbound FOSS Acquisition

Acquisition of Inbound FOSS must follow the rules established by TSS Now -- the Technology Strategies and Standards and the Asset Lifecycle Management (ALM) group.

7.3.2 Open Source Trials

If you want to acquire Inbound FOSS *solely to trial* and determine its fitness for your purpose, you are granted an automatic exception to this Policy's Section 7.1 above. Trials do not require the approval of the TSS or ALM but must meet the criteria specified by the Open Source First Team requiring simple registration for tracking purposes. (https://wiki.web.att.com/x/_SWbGQ)

7.3.3 License Options

Often, there is a choice between similar FOSS products. When there are competing FOSS product choices of similar function and quality, AT&T always prefers the products available under Permissive Licenses, not Copyleft Licenses.

AT&T Technology Policy**Freeware, Shareware, and Open Source Software (FOSS) Policy**

7.4 Outbound Code Contribution Rules**7.4.1 Code Scanning**

Software applications that AT&T intends to contribute to an open-source community, repository, or project **must** be scanned by AT&T internally approved scanning tools for security issues, FOSS code, other third-party code, or snippet identification, license attribution, and reporting, and provide an SBOM. All contributions must meet the open source community rules.

7.4.2 Open Source Code Scanning

Outbound contribution cannot contain FOSS for which AT&T cannot determine the license. Outbound FOSS may contain FOSS under a Copyleft License only if the open source community rules require it, and with approval from the AT&T Legal Department.

7.4.3 AT&T Exempt Employee Contributions to External or Internal Projects and Communities

An AT&T exempt employee, a salaried employee not having time reporting, is free to contribute to any existing FOSS project or community that is external to AT&T with prior approval from their supervisor.

7.4.4 AT&T Non-Exempt Employee Contributions

Non-exempt employees may not submit contributions without supervisor approval nor work on their own time to contribute FOSS to any project or community on the behalf of AT&T, including to AT&T-sponsored projects. If the contribution is made to benefit AT&T, non-exempt employees must do it during regular business hours and only with the approval of their supervisor.

7.4.5 Community Agreements and Membership

Many open-source communities require membership or an agreement to be in place before contributions are made. The Linux Foundation and the Apache Foundation communities are prime examples. If you want to participate in an open-source community and you wish to make contributions, it is your responsibility to ensure that membership agreements are in place with proper prior approvals through the [Open Source Process Center](#). You may NOT make any contributions to an open source community unless you have Open Source Process Center approvals including legal approval.

Blanket (standing) approvals to making contributions may be granted through [the Open Source Process Center](#) after membership to the open-source community is approved. Memberships to FOSS communities must be approved by the BU officer – Level 6, the Legal Department, and the Intellectual Property business unit.

AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

7.5 Outbound FOSS to Open Source Repositories (Contribution Types)







A light-touch review process is in place to approve contributions via the Open Source Process Center. A business unit need is required to release software as open-source software.

7.5.1 Open-Source Contribution Review and Approval

Before any code may be contributed to an open-source community or an external repository, the employee making the contribution must obtain approval via an Open Source Process Center (OSPC) request (see link provided below).

There are six (6) open-source contribution types that AT&T makes:

Open Source Software Contribution Types

	Contribution Types		Description
SIMPLE	Bug Fix		Minor fixes in OSS code.
	Enhancement/New Feature		Further development of code features.
COMPLEX	New OSS Project		Independent AT&T development.
	OSS Standards Participation		Participation in community development of code based on standards and shared goals: OpenStack, Apache Foundation, etc.
	Special Engagement		Special project participation with other companies, entities, or universities.
	Unclassified		One-off projects for particular technologies, such as ARO tool.

In the figure above, the contribution types identified in green refer to simple contributions made under a streamlined approval process requiring only a Level 3 approver. The types identified in blue require a more detailed review with a Level 5 BU approver, Legal, and the AT&T Intellectual Property business unit.

The [Open Source Process Center \(OSPC\)](#) request must be submitted before an open source contribution is made. The OSPC request automatically routes the request through the appropriate approval workflow.

7.5.1 Bug Fix

Bug fixes are defined as simple fixes to correct a defect in existing external FOSS. The goals of the bug fixes are to improve the AT&T ecosystem that may use the same FOSS across many business units. A bug fix does not introduce new functionality – thus,

AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

preventing the release of any AT&T intellectual property. Additional bug fixes need no new approval to the same FOSS.

7.5.2 New Feature/Enhancements

An enhancement/new feature is defined as functionality added to existing FOSS. When the enhancement/new feature does not competitively differentiate AT&T, it may be considered for contribution back to the open-source community as Outbound FOSS. An approval by a Level 3 BU representative via an OSPC request is required to externally contribute a new feature/enhancement. No new requests needed for same FOSS.

7.5.3 New Project

A new open source project is one which originated at AT&T with code written within or completely by AT&T or co-developed with an AT&T vendor. The Legal Department shall determine which FOSS license should be used via OSPC approval process. AT&T's GitHub organization is the preferred repository for new open-source projects.

7.5.4 OSS Standards Participation/Special Engagement/Unclassified

OSS Standards Participation, Special Engagements, and Unclassified (one-off) are all special arrangements that require review and approval from the AT&T business unit creating the code, Legal Department, and the Intellectual Property business unit. As described above, approval is granted via the OSPC request.

7.6 External Distribution of AT&T Applications and Code

Software written by AT&T, including Generative AI code, which is distributed or exposed externally must be scanned by an internal approved AT&T tool to identify whole FOSS modules, snippets of FOSS, or unidentified code contained in such software. All AT&T software distributed externally must be approved by the TSS Now process (which includes legal approval to ensure FOSS license terms compliance) and other software requirements by TSS Now. The software must use approved Artifacts and provide: an SBOM, License URL's, and the context of External Distribution such as mode of distribution: via an app store, SaaS, delivery of standalone software to an enterprise, AT&T Website, or delivery via an AT&T device such as home gateway or router. (See also TSS Now requirements in Section 7.1 above).

7.7 Vendor-provided Open Source Software

Frequently, software purchased or otherwise acquired through AT&T's vendors contains FOSS. Such FOSS may either be embedded in the vendor's product or provided along with the vendor's product.

AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

7.7.1 No TSS Now Approval Needed for Vendor Code:

Subject to Section 7.7.2 below, Vendor supplied software does not need TSS Now approval. Supply chain contracts cover FOSS requirements in the agreement. No permission is required from the TSS Now process when entering into such supply chain contracts.

7.7.2 Separate Use of Non-Embedded FOSS (Stand Alone FOSS)

FOSS provided by a vendor as stand-alone FOSS, alongside a vendor's product (as opposed to being embedded in the vendor's product), must be approved prior to use at AT&T by first obtaining an approved supply chain contract with the AT&T FOSS clause; or alternately obtaining a TSS Now process request to use such stand-alone FOSS.

7.7.3 Commercial Software Scans

AT&T may wish to scan, using an internal AT&T tool, commercial (vendor) software we acquire to identify the underlying open source software if a security or legal risk may be identified. The Software Bill of Materials (SBOM) may also be requested from the vendor. This SBOM may then be used to identify license or security issues not acknowledged by the vendor. Any such scanning must be done via an approved AT&T scanning tool.

7.8 Foss Resources

As AT&T continues to move towards using more FOSS, AT&T will increase the number of TSS standardized FOSS products at the AT&T internal repositories, including through AT&T vendor-provided resources. Software developers must look internally for FOSS products they wish to use before reaching out to GitHub or other approved AT&T repositories, or the web. Each resource must be identified in any TSS Now request. You should avoid bringing in unidentified code.

7.9 Employee Education and Compliance Obligations

All software developers working with FOSS are required to take the training course on Open Source Software (OSS) Licenses and Copyright available at the Learning Service Organization (LSO course # 61793745) as part of their Compliance Training. This is a mandatory requirement as part of employee compliance training.

8.0 Governance

The Open Source First Team is responsible for oversight of this FOSS Policy. Any changes to this Policy will be made by the CIO, CSO, and the Open Source First Team with approval from the Legal Department.

9.0 FOSS Policy Exceptions

If you feel that you have a valid business need that requires you to vary from this FOSS Policy, you may request an Exception to this Policy. To submit a TSS Now process request visit <http://att.sharepoint.com/sites/TSS> to complete and submit a request that provides details about your activity and why an exception to this Policy is required.



AT&T Technology Policy

Freeware, Shareware, and Open Source Software (FOSS) Policy

Submitting a TSS Now process request, however, does not mean that you can vary from this Policy. Your request will be evaluated by TSS Now to determine if a waiver is warranted. Until a waiver is obtained, you must continue to adhere to this Policy.

Policy Manager

Name: Kendal Miller

Phone: 404-786-5529

Email address: km850g@att.com

Approvals

Author(s): Kendal Miller, Jeff Harp, Umesh Desai

Reviewed by: Kendall Miller, Umesh Desai

Final Approval: CIO-TSS, CSO, Legal

Legal: Umesh Desai