

Third Party Licensing Uses

for



Version: 1.0

October 2024

(Privacy: Private)

DOCUMENT CONTROL



A. Document Information

Document Name	Third Party Licensing Uses
Document Number	BS23-QMS-PRO-37
Document Author	Head of Quality & Compliance (HQC)
Document Location and Access	This document will be maintained as an electronic copy in a storage/portal/file server and shared with the appropriate stakeholders according to the Document Distribution List by mail/portal/shared drive.
Document Control	This document is for the use of BS23. Any document sharing with external entities without the approval of the authority is strictly prohibited and is subjected to forward for disciplinary action for such activity. Any unauthorized modification is strictly prohibited. Please refer to the author/owner should there be any need for clarification or additional information about the document.
Document Classification	This document is classified as ' Private '. Information/ document could be used/ disclosed with authorized persons according to document classification.
Conformity	Any practice deemed required by the Regulatory Body, Government, Relevant standard/ frameworks/ directives, and Applicable Local/ International Laws will override the entire or any part mentioned in this document.
Recommendation	Users of this document are responsible for using only the latest version.
Enforcement	This document shall be released and come into force with effect from the date of Approval.
Retention & Disposition	<p>The obsolete version of the document will be retained and maintained according to the Retention Policy of BS23.</p> <p>The copies distributed among the users will be invalid immediately after the publication of the new version and respective department/Division/Branch Head will destroy the obsolete distributed.</p>
Review Frequency	This document and the content statements of the document will be reviewed as on a demand basis.

B. Document Distribution List

Serial No.	Person/ Department/ Designation/ Team
01	All Internal Stakeholders

C. Author Information

Prepared By		
Name	Designation	Signature
Md. Sazzad Munir	Head of Quality & Compliance	
Reviewed By		
Name	Designation	Signature
Mizanur Rahman	CTO	
Approved By		
Name	Designation	Signature
Raisul Kabir	CEO	

D. Document History

Version No	Revision Date	Approval Date	A/M/D/N	Description of Change	Document Author	Approved By
1.0	03.10.2024	03.10.2024	N	First Release	HQC	CEO

* A= Added, M= Modified, D= Deleted, N= New Published

Table of Contents

1	Purpose	5
2	Scope	5
3	Approved License Types	5
3.1	Permissive Licenses	5
3.2	Weak Copyleft Licenses	5
4	License Types Requiring Careful Consideration	5
4.1	Strong Copyleft Licenses	5
4.2	Other Licenses	6
5	Evaluation Criteria for Open-Source Software or Library	6
5.1	License Review	6
5.2	Security	6
5.3	Community and Maintenance	6
5.4	Compatibility and Integration.....	6
6	Attribution and Compliance.....	6
6.1	Giving Credit	6
6.2	Documentation	6
7	Approval Process.....	7
8	Policy Compliance.....	7
9	Review and Updates	7
10	References and Documents	7
10.1	References	7
10.2	Documents	7

1 Purpose

At Brain Station 23, we will use licensed and open-source software and libraries. This policy outlines the guidelines for selecting, using, and attributing open-source software and libraries (we will refer it as OSS in this document) within the organization to ensure compliance with legal, security, and operational standards.

2 Scope

This policy applies to all employees and contractors involved in software development, maintenance, or distribution within the organization.

3 Approved License Types

The following open-source licenses are generally approved for use within the organization:

3.1 Permissive Licenses

Permissive licenses allow maximum flexibility for use, modification, and distribution. They are typically preferred for use within the organization.

- **MIT License:** Allows commercial use, modification, distribution, and private use with minimal requirements (e.g., including the original license and copyright notice).
- **Apache License 2.0:** Allows commercial use, distribution, modification, and private use. Includes an explicit grant of patent rights from contributors.
- **BSD License (2-Clause, 3-Clause):** Similar to the MIT License, with minimal restrictions. The 3-Clause license includes an additional clause preventing endorsement by the original authors.

3.2 Weak Copyleft Licenses

Weak copyleft licenses require changes to the library itself to be open source but allow software that merely links to the library to remain proprietary.

- **GNU Lesser General Public License (LGPL):** Allows linking to the library in proprietary software, provided modifications to the LGPL-licensed library are made available under the same license.
- **Mozilla Public License (MPL) 2.0:** Similar to the LGPL, but applies on a file-by-file basis, making it more flexible for proprietary software integration.

4 License Types Requiring Careful Consideration

4.1 Strong Copyleft Licenses

Strong copyleft licenses require that any derivative work or software incorporating the licensed code be released under the same license, which can conflict with proprietary software development.

- **GNU General Public License (GPL) v2/v3:** Requires that any software incorporating GPL-licensed code also be released under the GPL. This can affect the ability to keep software proprietary.
- **GNU Affero General Public License (AGPL):** Similar to the GPL, but also requires making the source code available when the software is used over a network (e.g., SaaS applications).

Policy: Usage of software under these licenses requires explicit approval from the [Legal/Compliance Department] due to the impact on software distribution and intellectual property.

4.2 Other Licenses

- **Creative Commons Licenses:** Generally used for media and documentation, not software. Ensure that the specific Creative Commons license is suitable for the intended use.
- **Unlicensed Software:** OSS without a license should be avoided, as the legal terms are unclear.

5 Evaluation Criteria for Open-Source Software or Library

Before adopting any open-source software or library, the following parameters must be evaluated:

5.1 License Review

- Verify that the OSS license is listed in the approved license types.
- Check for restrictions on commercial use, distribution, modification, and patent rights.

5.2 Security

- Perform a security assessment, including vulnerability scanning.
- Evaluate the frequency of updates and the maintainer's response to security issues.

5.3 Community and Maintenance

- Evaluate the size and activity level of the software's community.
- Review the project's commit and release frequency to ensure active maintenance.
- Assess the quality of documentation and support channels (e.g., forums, mailing lists).

5.4 Compatibility and Integration

- Ensure the OSS is compatible with the organization's software stack.
- Review the dependencies to avoid additional risks.

6 Attribution and Compliance

When using OSS, comply with the attribution requirements specified in the license. Follow these guidelines:

6.1 Giving Credit

- **MIT License:** Include the license text and copyright notice in the software documentation.
- **Apache License 2.0:** Include a NOTICE file if the original software includes one, in addition to the license text.
- **LGPL/MPL:** Document any modifications to the library and include the license text.

6.2 Documentation

- Maintain a record of all OSS used, including version numbers and license types.
- Document any modifications to the OSS.

7 Approval Process

- Team members who identify the need for an open-source software or library, will reach out to the SBU head for approval of use. If this is already used in other places, then it is already approved.
- Upon approval from the SBU head, team members can use it. SBU head will record the OSS for future reference.
- The cases where the SBU head can't decide for approval based on the guidelines of this document, will consult the CTO for approval.

8 Policy Compliance

Non-compliance with this policy may result in disciplinary action and remediation to ensure compliance.

9 Review and Updates

This policy will be reviewed annually or as required to accommodate changes in open-source licensing, legal requirements, or organizational needs.

10 References and Documents

10.1 References

- ISO 9001:2015, Clause 8.4 – Control of externally provided processes, products and services

10.2 Documents

- List of approved third-party software or component