

Open Source Software (OSS) Acquisition Best Practices

Purpose

Carnegie Mellon encourages the use of open source software (OSS) to support research, teaching, and innovation. These best practices are intended to enable broad use while helping faculty and researchers navigate common considerations such as data use, licensing, and external obligations.

General Approach

In most cases, OSS may be used without prior review when:

- The software is used locally (e.g., laptop, workstation, or CMU-managed environment)
- The use is within the university
- The work does not involve restricted or regulated data

This covers the majority of research and instructional use cases.

Practical Expectations

Faculty and researchers are best positioned to evaluate the tools they choose. As part of normal due diligence:

- Review the OSS license, especially if reuse or sharing is anticipated
- Consider whether the tool is actively maintained and appropriate for the work
- Recognize that OSS is typically provided without warranties or guarantees

The goal is informed use and not exhaustive review.

Data Considerations

Data classification is often the most important factor in determining appropriate use:

- **Public data** - generally no additional restrictions
- **Private or restricted data** - may require approved environments or controls
- **Highly regulated data** - may limit tool or platform choices

When data sensitivity increases, additional care and potentially guidance is warranted. Additional information about data classifications is available at <https://www.cmu.edu/data/guidelines/data-classification.html>

External Obligations

OSS use should align with any applicable agreements, including:

- Sponsored research agreements
- Data use agreements (DUAs)
- Non-disclosure agreements (NDAs)
- Other third-party commitments

Particular attention should be given to:

- Data handling and confidentiality requirements
- Whether OSS license terms introduce sharing or disclosure obligations

Sharing and Distribution

Additional review may be appropriate when:

- Software or code is shared outside CMU
- OSS is incorporated into deliverables, tools, or services for external use
- Modifications to OSS may trigger license obligations (e.g., source code sharing)

Planning ahead in these cases helps avoid rework later.

Security and Reliability

Basic practices help reduce risk:

- Prefer well-established, reputable projects
- Check for recent updates and active maintenance
- Be aware of known vulnerabilities
- Avoid unverified or unknown sources

Some titles are already approved and available in the university's software catalog (<https://www.cmu.edu/computing/software/>).

If you don't see it there, reasonable judgment is expected.

When to Seek Guidance

Reaching out is recommended when:

- Working with restricted or regulated data
- Questions arise about OSS license terms or obligations
- Research is governed by external agreements
- Software will be distributed externally
- There is uncertainty about an appropriate path forward

Available Resources

Resources for additional guidance and support:

- CMU license guide
 - [Open Source License Comparison Grid](#)
- CURIOSS Licensing Resources for Academic OSPOs
 - https://curiooss.org/news/licensing_resources_for_academic-ospos/
- Open Source Security Foundation
 - [Open Source Security Foundation](#)

Available Support

Support is available across the university:

- **Open Source Programs Office (OSPO)**
 - <https://www.library.cmu.edu/services/ospo>
- **Computing Services**
 - <https://www.cmu.edu/computing/>
- **Information Security Office**
 - <https://www.cmu.edu/computing/safe/index.html>
- **Software Catalog and Request Process**
 - <https://www.cmu.edu/computing/software/>

Early consultation is encouraged when questions arise.

Key Takeaways

- Most OSS use is permitted without prior approval
- Data sensitivity and external obligations are the primary considerations
- Additional review is situational, not required by default
- Support is available and intended to enable progress, not delay it

Final Note

This guidance is designed to support responsible and efficient use of OSS across Carnegie Mellon. It does not replace existing policies or contractual obligations but provides a practical framework for navigating common scenarios