Code Intelligence Platform

ACCEPTABLE USE POLICY

Permitted & Prohibited Uses

Silicon Harbor Technologies, LLC

Charleston, South Carolina

Effective Date: March 16, 2026

ACCEPTABLE USE POLICY

Last Updated: March 16, 2026

ACKNOWLEDGMENT AND ACCEPTANCE

This Acceptable Use Policy ("AUP") governs your use of Enovari services. By accessing or using Enovari, you acknowledge that you have read, understood, and agree to be bound by this AUP.

Silicon Harbor Technologies reserves the right to modify this AUP at any time. Changes become effective upon posting to enovari.io/acceptable-use. Continued use of Enovari after changes are posted constitutes acceptance of the modified AUP. Material changes will be communicated via email to the primary account holder.

If you do not agree to this AUP, you must immediately cease using Enovari services and may terminate your account in accordance with the Master Services Agreement.

1. Permitted Uses

Customers may use Enovari for:

- Analyzing proprietary or open-source code for which Customer has legal rights
- Security auditing and vulnerability assessment of owned codebases
- Technical debt assessment and refactoring planning
- Dependency mapping and architecture visualization
- Code quality assessment and complexity analysis
- Educational and research purposes consistent with academic integrity

2. Prohibited Uses

Customers SHALL NOT use Enovari to:

2.1 Illegal or Harmful Activities

- Develop, distribute, or analyze malware, ransomware, or malicious code
- Create exploit code for unpatched vulnerabilities without authorization
- Reverse engineer or analyze third-party software without legal rights
- Violate export control laws or develop code for prohibited jurisdictions
- Facilitate fraud, identity theft, or financial crimes

2.2 Intellectual Property Violations

- Upload or analyze copyrighted code without authorization

- Circumvent license restrictions or DRM systems
- Extract proprietary algorithms from competitor products
- Violate open-source license terms (e.g., GPL non-compliance)

2.3 Privacy & Data Protection Violations

- Upload code containing personally identifiable information (PII) without consent
- Store credentials, API keys, or secrets in analyzed codebases
- Analyze healthcare/financial code containing protected data (PHI/PCI)
- Process EU citizen data in violation of GDPR requirements

2.4 Platform Abuse

- Attempt to reverse engineer or decompile the Enovari platform
- Perform security testing or penetration testing without written authorization
- Automate access beyond API rate limits or usage quotas
- Sublicense, resell, or white-label Enovari services without written agreement
- Create derivative products that compete with Enovari using platform insights

3. Content Restrictions

Customers must NOT upload or process:

- Classified, export-controlled, or defense-related code without proper authorization
- Code containing hardcoded credentials, private keys, or authentication tokens
- Proprietary third-party libraries or frameworks Customer does not own or license
- Obfuscated or deliberately malformed code designed to evade analysis
- Code that violates any applicable law, regulation, or industry standard

4. Enforcement & Remedies

Silicon Harbor reserves the right to:

- Immediately suspend access upon detection of prohibited use
- Terminate Customer accounts for repeated or egregious violations
- Report illegal activity to law enforcement or regulatory authorities
- Delete prohibited content without notice or liability
- Seek injunctive relief and monetary damages for policy violations

Customers remain liable for all activity under their accounts, including unauthorized use by employees or contractors.

This is a unilateral policy and does not require signature.

Acceptance is indicated by accessing or using Enovari services.