

## Recommended Secure Software Purchasing Contract Language

This sample contract Annex is intended to help enterprises negotiate secure commercial-off-the-shelf (COTS) software purchases. Most software contracts have focused on requiring the vendor to show a certain level of application security competency or to attempt to include liability clauses as part of the contract process. Frequently, the parties have very different views on what defines application security and what has actually been agreed to in the contract. The following language lays out a simple process, utilizing independent security reviews and industry standard benchmarks, which allows both vendors and enterprises to ensure that application security is embedded in the product.

Portions of this document incorporate details from the OWASP Secure Software Contract Annex and the SwA Working Group's "Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise" paper. Organizations are free to use the following sample language, however, as with any legal agreement, we recommend you contact a qualified attorney prior to entering into any contract.

### Sample Contract Annex

#### 1. INTRODUCTION

This Annex is made to \_\_\_\_\_ ("Agreement") between Client and Vendor. Client and Vendor agree to maximize the security of the software according to the following terms.

#### 2. ORIGIN, LIBRARIES, FRAMEWORKS, AND PRODUCTS

##### (a) Disclosure

Vendor shall disclose all binary executables (i.e. compiled or byte code; source code is not required) of the software, including all libraries or components.

##### (b) Origin

Vendor shall disclose the development origin of all software components used in the product.

#### 3. SECURITY REVIEWS

##### (a) Independent Review

Vendor shall have their software reviewed for security flaws, in binary format (i.e. compiled or byte code; source code is not required), by an independent organization that specializes in application security, at their expense, prior to delivery to the Client.

##### (b) Review Coverage

Security reviews shall cover all aspects of the software delivered, including third party components, and libraries.

##### (c) Scope of Review

At a minimum, the review shall cover common software vulnerabilities. The review may include a combination of static analysis of the binary code, dynamic web application vulnerability scanning, and manual penetration testing.

#### **(d) Issues Discovered**

Overall application security ratings with aggregate number of flaws found will be reported to both Client and Vendor. Detailed reports of specific vulnerability instances within the application will only be provided to the Vendor. All issues will be tracked and remediated as specified in the Security Issue Management section of this Annex.

#### **(e) Standard Benchmarks**

To ensure that all parties have a common understanding of any security issues uncovered, the independent organization that specializes in application security shall provide a rating based on industry standards as defined by First's Common Vulnerability Scoring System (CVSS) and Mitre's Common Weakness Enumeration (CWE).

#### **(f) Review Frequency**

Reviews shall be conducted to revalidate the software prior to delivery of any new major or minor release prior to delivery to Client.

### **4. SECURITY ISSUE MANAGEMENT**

#### **(a) Identification**

Vendor will track all security issues uncovered during the security review and the entire life cycle, whether a requirements, design, implementation, testing, deployment, or operational issue. The risk associated with each security issue will be evaluated, documented, and reported to Client as soon as possible after discovery.

#### **(b) Protection**

Vendor will appropriately protect information regarding security issues and associated documentation to help limit the likelihood that vulnerabilities in operational Client software are exposed.

#### **(c) Remediation**

Client and Vendor shall create a mutually agreed upon remediation roadmap to resolve security issues that are identified. Vendor shall make all commercially feasible efforts to fix all high level issues prior to delivery to Client.

### **5. SECURITY ACCEPTANCE AND MAINTENANCE**

#### **(a) Acceptance**

The software shall not be considered accepted until the independent review is complete and all security issues have been assigned to a mutually agreed upon remediation roadmap.

#### **(b) Investigating Security Issues**

After acceptance, if security issues are discovered or reasonably suspected, Vendor shall assist Client in performing an investigation to determine the nature of the issue.

#### **(c) Other Security Issues**

Vendor shall use all commercially reasonable efforts consistent with sound software development practices, taking into account the severity of the risk, to resolve all security issues as quickly as possible.