

Supplier Policy
Information Security Requirements
(Software Development)

C1 Public

SCOPE

One New Zealand (One NZ) maintains a number of One NZ Supplier Policies used in all One NZ procurement agreements with suppliers.
In addition to the One NZ Supplier Policy – Information Security and Minimum Security Requirements Schedule outlined in supplier contracts, One NZ has further information security requirements applicable for all One NZ procurement agreements where the Supplier will be providing Software Development Services.

1 POLICY

1.1 Introduction

This Policy outlines the minimum information security requirements for external suppliers providing software development services to One NZ. Suppliers are required to adopt secure development practices aligned with recognised industry standards to ensure the protection of One NZ information.

Upon request, Supplier shall provide to One NZ for review and approval: (i) Secure Coding Guidelines to be followed by all its software developers aligned with recognised industry standards (including but not limited to OWASP SAMM, NIST SSDF, ISO 27034, or an equivalent framework); and (ii) Penetration Security Test procedures for major software point releases.

1.2 Supplier Requirements

Supplier shall ensure that:

1.2.1. It appoints an Information Security Personel responsible for monitoring and enforcing compliance with One NZ's information security requirements;

1.2.2. Its software developers comply with the Secure Coding Guidelines referred to above;

1.2.3. All software developers providing Software Development Services to One NZ are fully trained on industry recognised secure coding practices;

1.2.4. It stores all code in a secure and restricted location;

1.2.5. It makes a back-up of all code;

1.2.6. All code has been reviewed by more than one software developer, and the review process has been documented;

1.2.7. The code is tested for inclusion of any One NZ security requirements and against the OWASP Top 10;

1.2.8. All third-party software code is formally tested and approved before being used within any One NZ applications;

1.2.9. All security flaws in the code are resolved to One NZ's satisfaction at Supplier's expense within an agreed timeframe;

1.2.10. It provides One NZ with detailed release notes explaining what security vulnerabilities have been mitigated per release and guidelines on how to deploy;

1.2.11. It provides One NZ with summary results of the Penetration Security Tests conducted for all major software point releases; and

1.2.12. All security vulnerabilities identified within software releases are corrected within a reasonable timeframe agreed with One NZ.

C1 Public

1.2.13. They have a process in place to manage software development risks associated with their own third-party vendors and partners.

1.3 Reporting

Supplier shall provide a report on its compliance with this One NZ Supplier Policy upon request from One NZ including relevant supporting evidence.

2 DEFINITIONS AND INTERPRETATION

The following words and expressions have the following meanings in this document:

"OWASP Top 10"	The top 10 most critical security risks to web applications based on broad consensus from the industry[1]
"Software Development Lifecycle (SDLC)"	means is a structured process that guides the planning, development, testing, deployment, and maintenance of software systems.
"Software Development Services"	means the provision of software/ application development and associated services such as testing, quality assurance and release management.
"NIST SSDF (Secure Software Development Framework)"	means a set of high-level, outcome-based secure software development practices designed to be integrated into the SDLC to reduce vulnerabilities and improve software security.
"Minimum Security Requirements Schedule"	means the One NZ Minimum Cyber Security Requirements Schedule, which sets out the baseline security controls applicable to all Suppliers accessing or handling One NZ information, forming part of the contractual security obligations.

The phrase "Supplier" in this Supplier Policy shall, where relevant, also include all officers, employees, contractors, subcontractors and agents of Supplier.

[1] Ref: https://owasp.org/www-project-top-ten/

C1 Public