# Supplier Policy
# Information Security Requirements
# (Software Development)

## SCOPE

One New Zealand 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, One NZ has some additional information security requirements for all One NZ procurement agreements where the Supplier will be providing Software Development Services.

## 1 POLICY

### 1.1 Documentation

Supplier shall provide to One NZ for review and approval: (i) Secure Coding Guidelines to be followed by all its software developers; and (ii) Penetration Security Test procedures for major software point releases.

### 1.2 Security requirements

Supplier shall ensure that:

1.1.1. It appoints a Security Officer responsible for monitoring and enforcing compliance with One NZ's information security requirements;
1.1.2. Its software developers comply with the Secure Coding Guidelines referred to above;
1.1.3. All software developers providing the Software Development Services to One NZ are fully trained on industry recognised secure coding practices;
1.1.4. It stores all code in a secure and restricted location;
1.1.5. It makes a back-up of all code;
1.1.6. All code has been reviewed by more than one software developer and the review process has been documented;
1.1.7. The code is tested for inclusion of any One NZ security requirements and against the OWASP Top 10 ;
1.1.8. All third-party software code is formally tested and approved before being used within any One NZ applications;
1.1.9. All security flaws in the code are resolved to One NZ's satisfaction at Supplier's expense within an agreed timeframe;
1.1.10. It provides One NZ with detailed release notes explaining what security vulnerabilities have been mitigated per release and guidelines on how to deploy;
1.1.11. It provides One NZ with summary results of the Penetration Security Tests conducted for all major software point releases; and
1.1.12. All security vulnerabilities identified within software releases are corrected within a reasonable timeframe agreed with One NZ.

### 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 Services" | means the provision of software/ application development and associated services such as testing, quality assurance and release management. |

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/