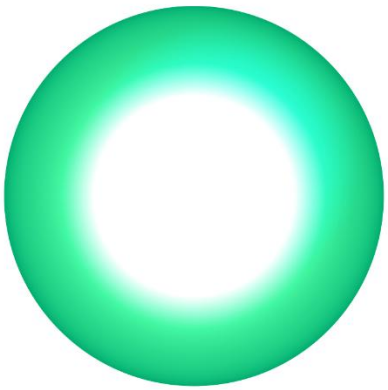

Supplier Policy
Supplier Security Risk Management

SCOPE

All One New Zealand procurement contractual agreements with Suppliers.

1 POLICY

1.1 Introduction

One New Zealand ("One NZ") is committed to protecting the confidentiality, integrity, and availability of information entrusted to us by our customers, employees, partners, and stakeholders. As part of this commitment, One NZ requires all suppliers to maintain a Supplier Security Risk Management Program to identify, assess, manage, and monitor security risks associated with and the suppliers' third (fourth, etc.) parties that process, store, transmit, or access One NZ information and/or systems.

The purpose of this policy is to establish the principles and requirements used to evaluate and manage supplier security risks throughout the supplier lifecycle, including sourcing, onboarding, ongoing engagement, and contract termination.

The program must be designed to:

- Protect One NZ information and assets from unauthorized access, disclosure, alteration, destruction, or loss.
- Ensure suppliers maintain security controls appropriate to the sensitivity and volume of information they handle.
- Support compliance with applicable legal, regulatory, contractual, and privacy requirements.
- Monitor and manage supplier security risks throughout the duration of the supplier relationship.

1.2 Supplier Requirements

Suppliers must ensure that their third (fourth, etc.) parties implement and maintain security controls appropriate to the services they provide One NZ, and the information they access, process, store, or transmit on behalf of One NZ.

At a minimum, all suppliers are expected to:

- Protect the confidentiality, integrity, and availability of One NZ information through appropriate technical and organisational controls.
- Restrict access to authorised personnel and maintain effective identity and access management practices.
- Maintain security operations, including vulnerability management, monitoring, and incident response capabilities.
- Apply secure-by-design principles throughout the development, deployment, and maintenance of technology solutions where applicable.
- Promptly notify One NZ of any actual or suspected security incident impacting One NZ information, systems, or services within 72 hours of discovery and take appropriate remediation actions to mitigate the impact and prevent recurrence.
- Ensure subcontractors and downstream service providers maintain equivalent security standards where they support the delivery of services to One NZ.
- Provide reasonable assurance of their security controls through certifications, assessments, audits, or other evidence when requested.

1.3 Risk Assessment and Monitoring

A risk-based approach should be applied to supplier security management where suppliers servicing One NZ should be subject to security assessments before engagement and periodically throughout the relationship.

Recommended risk-based approach:

2 DEFINITIONS AND INTERPRETATION

In this One NZ Supplier Policy on Supplier Security Risk Management and in its application, the following words and expressions shall have the meanings set out below.

"Supplier"	Any organization or individual providing products, services, systems, or support to One NZ, including subcontractors and outsourced service providers.
"Confidential Information"	Information classified as confidential or higher under One NZ's information classification framework, including customer, employee, commercial, financial, and strategic information.
"Personal Information"	Information relating to an identified or identifiable individual, including customer, employee, contractor, and partner information.
"Supplier Security Risk"	The potential impact arising from inadequate security controls, vulnerabilities, incidents, or other security weaknesses associated with a supplier's products, services, systems, personnel, or subcontractors.
"Risk Assessment"	A structured evaluation performed to determine the security risk associated with a supplier, taking into consideration the nature of the service, information handled, security controls implemented, and overall risk exposure.