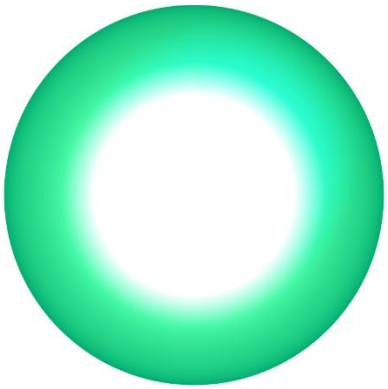


Supplier Policy
Information Security Requirements
(Remote Access)

C1 Public

SCOPE

One New Zealand (One NZ) maintains a number of Supplier Policies used in all One NZ procurement agreements with suppliers.

In addition to the One NZ Supplier Policy – Information Security, One NZ has additional information security requirements for all One NZ procurement agreements where the Supplier will need Remote Access.

1 POLICY

1.1 Introduction

This Policy defines the minimum information security requirements for external suppliers who require remote access to One NZ systems, networks, or data in order to deliver contracted services.

One NZ recognises that remote access introduces elevated security risks due to the connection of external environments to internal systems. Therefore, suppliers must implement and maintain appropriate controls to ensure that access is strictly limited, securely managed, and aligned with One NZ's cyber security standards and contractual obligations.

1.2 Supplier Requirements

Supplier shall ensure that:

1.2.1. Use Remote Access only to the minimum extent necessary in order to perform the contracted services;

1.2.2. Request Remote Access Credentials only for those Supplier personnel essential to the performance of the services;

1.2.3. Store Remote Access Credentials in secure locations accessible only to authorised Supplier personnel;

1.2.4. Ensure that Supplier personnel keep confidential and do not share their individual Remote Access Credentials with others;

1.2.5. Notify One NZ when Supplier personnel no longer require Remote Access and therefore that Remote Access Credentials should be disabled. Keeping copies of any One NZ data is prohibited.

1.2.6. Provide One NZ (on request) with lists of all Supplier personnel with Remote Access; and

1.2.7. Make sure that all relevant Supplier Personnel are aware of and comply with this One NZ Supplier Policy.

1.2.8. All data transmitted between Supplier systems and One NZ during remote access must be encrypted using industry-standard encryption protocols. This ensures that data remains secure during transmission.

1.2.9. In the event of a data breach during remote access, Supplier personnel must immediately report the incident to the One NZ Cyber Defence Centre (CDC) using cdc@one.nz .The report should include details of the breach, the data affected, and the steps taken to mitigate the impact.

1.2.10. Upon termination or expiry of the supplier's services, the Supplier must ensure the following:

- All remote access to One NZ systems, networks, and data must be immediately disabled and securely revoked for all supplier personnel, including service and privileged accounts.
- All credentials (e.g., usernames, passwords, API keys, certificates, tokens) issued for remote access must be securely removed, revoked, or invalidated.

C1 Public

- Any network connectivity configurations established for remote access (e.g., VPN tunnels, IP allow-listing, firewall rules, access gateways) must be removed or disabled.
- Any Supplier-managed devices that were used for remote access must no longer retain any One NZ data, configurations, or access artefacts.

If Supplier breaches the obligations in this policy, One NZ has the right to audit Supplier (up to a maximum of once per year).

2 DEFINITIONS AND INTERPRETATION

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

"Remote Access"	means the ability to connect to the One NZ network and/or systems from a distant location and separate network;
"Remote Access Credentials Review"	a review to ensure that only necessary Supplier personnel have Remote Access;
"Remote Access Credentials"	means the pins, passwords, access codes, access fobs and other similar credentials used to enable Remote Access;

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

C1 Public