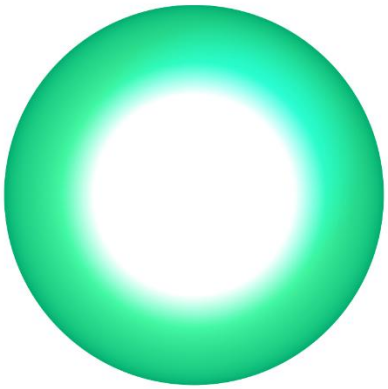


Supplier Policy
Information Security

C1 Public

SCOPE

All One New Zealand (One NZ) agreements with Suppliers.

Note: Compliance with the One NZ Minimum Security Requirements Schedule is contractually required and applies to all Suppliers who access, process, store, or transmit One NZ information or provide services to One NZ.
This policy sets out additional baseline information security obligations that apply to Suppliers throughout the duration of the engagement.

1 POLICY

1.1 Introduction

One NZ is committed to protecting its information assets and ensuring that appropriate information security controls are maintained across its supply chain. As external suppliers may access, process, store, or transmit One NZ information, they play a critical role in maintaining the confidentiality, integrity, and availability of that information.

This External Supplier Information Security Policy requires all suppliers to implement and maintain robust security controls, demonstrate compliance with applicable legal, regulatory, and contractual obligations, and cooperate with One NZ in the assessment and management of risks. These requirements extend not only to the supplier but also to any subcontractors or third parties engaged in delivering services to One NZ.

1.2 Supplier Requirements

Supplier shall:

1.2.1. Maintain an information security program aligned with recognised industry standards (e.g., ISO 27001, NIST CSF, SOC 2) and provide evidence of such compliance upon request.
1.2.2. Promptly and accurately complete and return any One NZ Supplier Security Risk Assessment whenever requested by One NZ;
1.2.3. Promptly respond to, and provide copies of, Information Security documentation, service designs and architecture, certifications and reports, when requested by One NZ;
1.2.4. Safeguard the security of all One NZ Confidential Information (such phrase in this policy shall have the meaning given in the supplier agreement), using appropriate technical and organisational security systems and processes reasonably acceptable to One NZ as per the Minimum Security Requirements Schedule;
1.2.5. Perform regular and full testing procedures on such security systems and processes;
1.2.6. Permit One NZ, upon reasonable notice to the Supplier, to conduct security audits against such security systems and processes (including the right to test the security of any hardware and software used by Supplier in the performance of its obligations under the supplier agreement);
1.2.7. Take all appropriate steps, including technical and organizational steps, to mitigate identified security weaknesses;
1.2.8. Not reduce the security levels associated with such security systems and processes without One NZ's prior written consent; and
1.2.9. Agree with One NZ on any changes to the security controls prior to the implementation; and
1.2.10. Notify One New Zealand's Cyber Defence Centre (CDC) by email at cdc@one.nz immediately (as agreed contractually) after becoming aware of a data breach or an incident where any One NZ information is at risk of unauthorised or unlawful disclosure, loss or damage.
1.2.11. Provide such assistance as One NZ may reasonably require to all security and fraud investigations in connection with the services provided.

C1 Public

1.2.12. Supplier shall ensure subcontractors and critical upstream providers meet equivalent information security requirements, remain responsible for their performance, and maintain a current register of such dependencies.

1.2.13. Supplier shall notify One NZ in advance of onboarding or changing any subcontractor that may access One NZ information or systems, and shall obtain One NZ's prior written approval where required.

1.2.14. Not use One NZ data (including metadata) to build, train, test, improve, or adjust Artificial Intelligence (AI) or machine learning systems unless you first get written approval from both the One NZ Privacy Officer and the Chief Information Security Officer (CISO).

1.2.15. Upon expiry or termination, Supplier shall return all One NZ data in a One NZ-approved format and securely delete any remaining copies, providing a certificate of destruction/erasure. Where cloud is used, exit/transition must follow One NZ's cloud exit requirements. All suppliers with access to One NZ data must complete the One NZ Supplier End of Service (EoS) Security Assessment.

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:

"EoS Security Assessment"	means the formal security review conducted upon the termination, expiry, or transition of a Supplier's services to One NZ, to verify that all information security obligations have been fulfilled. This includes confirming the secure return, transfer, or destruction of One NZ information, and the revocation of all physical and logical access to One NZ systems and data.
"One NZ 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.

C1 Public