Supplier Policy
Information Security

C2 General

Supplier Policy

Information Security

SCOPE

All One New Zealand agreements with Suppliers.

1 POLICY

1.1 Introduction

Supplier shall:

1. Promptly and accurately complete and return any One NZ Information Security Assessment Questionnaire whenever requested by One NZ;
2. Promptly respond to, and provide copies of, Information Security documentation, service designs and architecture, certifications and reports, when requested by One NZ;
3. 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;
4. Perform regular and full testing procedures on such security systems and processes;
5. 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);
6. Take all appropriate steps, including technical and organizational steps, to mitigate identified security weaknesses;
7. Not reduce the security levels associated with such security systems and processes without One NZ's prior written consent; and
8. Agree with One NZ on any changes to the security prior implementation; and
9. Notify One New Zealand's Cyber Defence Centre 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.
10. Provide such assistance as One NZ may reasonably require to all security and fraud investigations in connection with the services provided.
11. 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.
12. 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.
13. 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 and all suppliers with access to One NZ data must complete the One NZ Supplier End of Service 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).

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

C2 General