

Supplier Policy
PCI Compliance

C1 Public

SCOPE

All One New Zealand (One NZ) procurement agreements with Suppliers that involve payment cards.

1 POLICY

1.1 Introduction

This One NZ Supplier Policy on Payment Card Industry (PCI) Compliance: (i) sets out Supplier's obligations for data security for cardholder data; and (ii) is additional to Supplier's obligations in relation to data processing and minimum-security requirements.
In this One NZ Supplier Policy on PCI Compliance: (i) all obligations on Supplier shall be interpreted as being obligations not just on Supplier, but obligations on Supplier to procure compliance with the same obligations by its sub-contractors and agents; (ii) where Supplier is under an obligation it shall bear all of the costs of compliance with the obligation; and (iii) where Supplier has an obligation to provide information then it shall do so as soon as reasonably practicable.

1.2 Supplier Requirements - PCI Data Security

1.2.1 Supplier shall: (i) handle and store cardholder data in accordance with this One NZ Supplier Policy on PCI Compliance; (ii) facilitate payment card transactions for no purpose other than those expressly agreed in writing by One NZ; (iii) comply with the most current versions of the PCIStandards available from time to time at http://www.pcisecuritystandards.org; (iv) ensure that its payment systems, networks, applications and payment transaction devices are compliant with the applicable PCI Standards.

1.2.2 In the event that the PCI Standards provide for choices or alternatives as to compliance then Supplier shall comply with all reasonable requests made by One NZ as to these choices or alternatives.

1.3 PCI Compliance Artefacts

1.3.1 Upon request, Supplier shall provide One NZ with full copies of the following artefacts required under PCI (depending upon the appointed Service Provider Level). These artefacts shall be prepared and submitted in accordance with the current version of the Payment Card Industry Data Security Standard (PCI DSS). The Supplier shall ensure that any updates to the PCI DSS are reflected in its compliance activities and documentation.

a) Annual Report on Compliance
b) Annual Self-Assessment Questionnaire
c) Attestation of Compliance
d) Quarterly ASV Network Scan

1.3.2 Supplier shall provide One NZ with written information detailing all applicable PCI DSS requirements, to the extent the supplier handles, has access to, or otherwise stores, processes or transmits the One NZ's cardholder data or sensitive authentication data, or manages the One NZ's cardholder data environment. This shall be provided on an annual basis or if the supplier's responsibilities change.

1.3.3 Supplier shall promptly notify One NZ in writing as soon as reasonably possible of becoming aware of any material change that may impact its PCI DSS compliance status. This includes, but is not limited to: (i) changes to systems, processes, or infrastructure involved in storing, processing, or transmitting cardholder data; (ii) engagement of subcontractors or third parties that may access cardholder data; or

C1 Public

(iii) any change in the Supplier's PCI Service Provider Level or compliance certification status.

1.3.4 One NZ shall have the right to perform a due diligence audit on Supplier to validate the results of each of the above artefacts.

1.4 PCI Compliance - Incident Management

1.4.1 Supplier shall notify One NZ in writing as soon as reasonably possible if it knows or suspects that cardholder data has been breached or used: (i) without authorisation; or (ii) contrary to its contractual arrangements with One NZ including this One NZ Supplier Policy on PCI Compliance. These matters are referred to in this One NZ Supplier Policy on PCI Compliance as "Incidents".

1.4.2 In relation to each Incident, Supplier shall: (i) provide, in a secure manner, to One NZ, all relevant cardholder account numbers; (ii) undertake its own audit in relation to the Incident and ensure that such audit identifies the root cause of the Incident and confirms whether or not Supplier was in compliance with the PCI Standards at the time of the Incident; (iii) provide to One NZ copies of all relevant audit and other similar reports in relation to the incident; (iv) be responsible for and pay all reasonable costs associated with the engagement of forensic investigation services by One NZ in accordance with the relevant Payment Card Industry and One NZ's own forensic procedures; (v) provide One NZ and its forensic investigators and auditors such waivers as are necessary to facilitate such forensic investigation services; and (vi) provide full cooperation and access to enable such forensic investigation services.

1.4.3 Supplier shall: (i) rectify all issues arising from an Incident; (ii) consult with One NZ about One NZ's communications to card holders affected by the Incident; (iii) provide to One NZ all relevant information (and associated waivers) to verify Supplier's ability to prevent future data incidents in a manner consistent its contractual arrangements with One NZ including this One NZ Supplier Policy on PCI Compliance; and (iv) compensate One NZ for any losses incurred by One NZ arising from fraudulent transactions, to the extent that such transactions result from Supplier's non-compliance its contractual arrangements with One NZ including this One NZ Supplier Policy on PCI Compliance.

1.5 PCI Compliance - Upon Termination

1.5.1 Following termination of the relevant contractual arrangement with One NZ, Supplier shall securely dispose of any cardholder data in its possession in accordance with any reasonable request by One NZ.

C1 Public

2 DEFINITIONS AND INTERPRETATION

In this One NZ Supplier Policy on PCI Compliance and in its application, the followings words and expressions shall have the following meanings:

"ASV"	means Approved Scanning Vendor, being a Supplier approved by the PCI SSC to conduct external vulnerability scanning services;
"Attestation of Compliance"	means a Statement of PCI compliance as completed by a Supplier in conjunction with either (i) an ROC; or (ii) an SAQ;
"PCI Standards"	means the standards published by the PCI Security Standards Council (PCI SSC) which covers the security of systems and networks that store, process, or transmit cardholder data. (a list of such standards and guidance being available at https://www.pcisecuritystandards.org/
"RoC"	means a Report on Compliance, being a detailed report containing information documenting an entity's compliance status with the PCI Standards;
"SAQ"	means a self-assessment questionnaire;
"Service Provider Level"	means the appropriate accreditation level of a Supplier as defined by the PCI SSC who carries out the processing, storage, or transmission of cardholder data.

C1 Public