Vector Group cyber security policy for third parties

1. Scope

1.1 This policy applies to all third parties that provide software, services or other deliverables, whether these are provided on-premises or as a cloud-based solution (**Services**) to the Vector Group.

1.2 There are three sections to this policy:

(a) **Section I:** All third parties must comply with section I;

(b) **Section II:** Third parties with formal attestation or certification against international accepted information security standards, may elect to comply with section II;

(c) **Section III:** Any third party that does not comply with section II must comply with section III; and

1.3 This policy applies in addition to any agreement (**Agreement**) between you and a member of the Vector Group. If there is a conflict between the terms of an Agreement and the terms of this policy then, to the extent of the conflict, priority will be given to the terms of the Agreement.

1.4 Vector may change this policy at any time by updating its policy on Vector's website. Where we have updated contact details for you, we will also provide written notice to you of such change.

1.5 In this policy:

Good Practice means the skill, diligence, care and foresight expected of a highly skilled and experienced person in the same or similar circumstances.

Malicious Code means any virus, bomb, Trojan horse or other malicious software or computer programming code that could impair, deny or otherwise adversely affect the Services, you, us or any Vector Data or Vector Systems.

Related Company has the same meaning as specified in section 2(3) of the Companies Act 1993 as if "company" includes a company or other body corporate incorporated or constituted in New Zealand or any other jurisdiction.

Security Incident means the unauthorised access, use, alteration or destruction of any Vector Data or Vector Systems, or other compromise or breach of your or our electronic or physical security.

Security Vulnerability means a weakness at the network, operating system, database or application software level, or within associated functions (such as a physical vulnerability at the location where Vector Data is stored), that could allow a Security Incident to occur.

Vector means Vector Limited or in relation to an Agreement, the member of the Vector Group that is a party to that Agreement.

Vector Data means all data, information, text, drawings and other materials in any form that a Vector Group member provides to you, or that you generate, collect, process, hold, store or transmit in connection with an Agreement, excluding Your Materials.

Vector Group means Vector Limited and each of its Related Companies.

Vector Systems means the electronic information systems including hardware, equipment, software, peripherals and communications networks owned, controlled, operated or used by the Vector Group.

We, **us** and **our** means Vector.

Your Materials means all software, documents and other materials created or owned by you or a third party independent of an Agreement, which are provided to Vector by you or on your behalf.

Section I – Policy requirements applicable to <u>all</u> third parties

2. Security incidents

2.1 If you become aware of a Security Incident that has or may significantly impact the delivery of any Service, or the confidentiality of Vector Data or the integrity of Vector Systems, you must:

(a) notify us within 24 hours of becoming aware of the incident;

(b) promptly, within 48 hours after first notification, provide any additional information we reasonably request in relation to the incident, its manner of introduction and the impact that the incident had/is likely to have;

(c) provide regular status updates for the incident until resolved; and

(d) provide as soon as practicable, but in any event within 7 days following resolution of the incident, a written report including (1) the date the incident occurred; (2) the length of any outage; (3) a summary of the incident; (4) details such as how/when the incident was detected, what was impacted, and any containment strategies; (5) the root cause of the incident; and (6) what corrective action was taken to prevent reoccurrence.

2.2 If we determine that other measures are required to contain, respond to or remediate a Security Incident (such as notice, credit monitoring services, fraud insurance or the establishment of a call centre to respond to customer inquiries) you will undertake those remedial actions and will bear the cost of doing so if the incident was caused by your negligence, failure to follow your processes, or failure to comply with this policy or an Agreement, or any other act or omission by you (whether or not intentional).

2.3 You must treat the occurrence and impact of any Security Incident as confidential. If you are required by law to disclose any details of a Security Incident, you must, unless prohibited from doing so by applicable law, immediately notify us and, unless you have our prior written consent, you must only disclose the minimum required by law.

3. Protection of Vector Data

3.1 Vector Data is confidential to Vector. You must not access, store or use Vector Data except as required to perform your obligations under an Agreement. Vector Data may not be incorporated into a Generative AI tool, without our prior written consent.

3.2 Where Vector Data includes personal information (as defined in the Privacy Act 2020 or any successor legislation), you must hold and process that personal information in accordance with our obligations under the Privacy Act 2020 or any successor legislation and our privacy statement, available at https://www.vector.co.nz/privacy-policy.

If you supply software or provide software development services to the Vector Group you must also comply with clauses 4 and 5.

4. Malicious Code and Security Vulnerabilities

4.1 As a provider of software or software development services, you must take all precautions in accordance with Good Practice necessary to prevent the introduction of Malicious Code and Security Vulnerabilities that impact Vector Data or Vector Systems, including:

(a) using best endeavours to ensure that, when you provide us with software, it does not contain any Malicious Code or Security Vulnerabilities and that you do not otherwise introduce Malicious Code or Security Vulnerabilities into any Vector Systems; and

(b) taking appropriate action when a Security Incident occurs, or Malicious Code or Security Vulnerabilities are discovered, such as quarantining the affected file, code, or hardware or software component (where applicable).

4.2 If you become aware of any Security Incident that involves the discovery or introduction of Malicious Code or Security Vulnerabilities, you must:

(a) identify the Malicious Code or Security Vulnerabilities and the corrective actions required to contain and resolve the incident;

(b) provide us with a software patch to fix, remedy, or remove the Malicious Code or Security Vulnerability as soon as reasonably practicable and in any case within one month or such other timeframe as we agree;

(c) if requested by us, take all necessary and reasonable corrective action to eliminate the Malicious Code or Security Vulnerabilities and prevent reoccurrence (including

implementing appropriate processes to prevent further occurrences) and rectify any consequence capable of rectification; and

(d) if the Malicious Code or Security Vulnerabilities cause a loss of operational efficiency or loss of data, provide all necessary assistance that we request to mitigate the losses and restore the efficiency and/or data as quickly as practicable.

5. Testing

5.1 Before providing any software to us you must run your own tests using the most recent version of a reputable, commercially available software program to ensure, to the extent possible, that the software:

(a) meets the requirements of the applicable Agreement;

(b) does not contain any Malicious Code or Security Vulnerabilities; and

(c) will pass any acceptance testing conducted under that Agreement.

5.2 If you fail to run such tests then, without limiting our other rights or remedies, you must cooperate fully with us and reimburse all reasonable costs incurred by Vector in relation to that failure, including for eliminating or reversing any adverse effects of any destructive element.

Section II

6. Third parties with formal attestation or certification

6.1 You do not need to comply with section III if you hold the following attestation or certification and comply with this section II:

(a) ISO/IEC 27001:2022 certification;

(b) ISO/IEC 27001:2013 certification, provided you are transferring from ISO/IEC 27001:2013 to ISO/IEC 27001:2022; or

(c) Current SOC2 type 2.

6.2 To satisfy Vector's cyber security requirements, the Services you provide to Vector must be within the scope of the attestation or certification you are relying on and you must provide to us the following documentation as evidence of this.

(a) ISO/IEC 27001 certification:

(i) the current ISO/IEC 27001 certificate that is not older than 12 months; and

(ii) the Statement of Applicability that is referenced on the certificate; or

(b) SOC2 type 2:

(i) the latest SOC2 type 2 report that is not older than 12 months; and

(ii) evaluates how you have designed and implemented your protective controls as defined in the AICPA Trust Service Criteria; and

(c) any other additional information that we may reasonably request from you to evidence your implementation of the protective controls referred to in such Statement of Applicability or SOC2 Type 2 report.

6.3 You must:

(a) maintain the formal attestation or certification that you have provided us evidence of in compliance with this section II; and

(b) on an annual basis, provide the respective documentation listed in clause 6.3.

6.4 If the attestation or certification you have submitted to us pursuant to this section II lapses, section III applies.

Section III – Policy requirements applicable to all third parties who do not comply with section II

7. Security Requirements

7.1 As a supplier of Services to Vector you must apply Good Practice to:

(a) continually assess your cyber risk;

(b) apply effective security controls and formal cyber risk governance processes to protect you and us from cyber threats;

(c) implement appropriate security controls that consider your and our cyber risk and, without limitation, to ensure that the bypassing of a single control or protection does not result in a Security Incident;

(d) ensure that your employees have the right level of cyber security awareness required to carry out their roles and responsibilities;

(e) use appropriate technologies, processes and procedures to address current and emerging cyber threats, and maintain a consistent baseline of controls to detect, prevent and respond to those threats; and

(f) apply any learnings from a Security Incident to improve cyber defences.

7.2 You must use reasonable, appropriate and adequate administrative, technical, procedural and physical safeguards in accordance with Good Practice to detect and prevent unauthorised use of, or access to, the Services, Vector Data and Vector Systems.

7.3 Without limiting your obligations under clause 7.2 you must apply Good Practice to:

(a) use and regularly monitor logical access controls with appropriate levels of identification, authorisation, authentication, and traceability to restrict access to the Services and Vector Data to only those individuals who require access to meet your obligations under an Agreement, and ensure that those controls are updated when individuals change roles or leave;

(b) enforce a password policy that meets or exceeds Good Practice with regards to password management;

(c) prohibits the use of generic user IDs and shared passwords by your users who access the Services, Vector Data and Vector Systems;

(d) implement multi-factor authentication for all remote access and privileged or administrative accounts;

(e) implement appropriate controls to detect and prevent Malicious Code or other Security Vulnerabilities on your own systems, and ensure that any third party systems that you use to provide the Services and to communicate with Vector Data or Vector Systems do so;

(f) promptly apply security measures and patches designed to address Security Vulnerabilities in accordance with the recommendation of the supplier of hardware or software that you use to provide Services to us;

(g) detect, prevent and monitor actual or suspected security breaches on any network, infrastructure or systems that you use to provide Services to us, and document and regularly test a formal process for responding and recovering from such events;

(h) ensure that your staff are trained in and understand (1) your information security policies, procedures and responsibilities, including those specifically related to providing Services to us; and (2) the importance of maintaining the confidentiality of Vector Data;

(i) regularly monitor the security of any network, infrastructure and systems that you use to provide Services to us and promptly report to us on any events, impacting Vector, as described in clause 2;

(j) implement secure coding policies and practices that are followed by all employees and contractors that you use to provide coding Services to us. We may require you to provide evidence of the effective implementation of these standards including the results of any quality assurance, testing and change and release management; and

(k) ensure that any remote connection to Vector Systems is secure and complies with any specific security requirements that we notify you of for third party connections, including when you connect using an interface or specification we provide.

8. Information security assurance

8.1 If you generate, collect, process, hold, store or transmit Vector Data or have access to any Vector Systems:

(a) we may require you to provide a written report summarising the result of any technical security assessment, for example penetration testing, which is relevant to the Services and any risks identified during the security assessment, including:

(i) a description of identified Security Vulnerabilities;

(ii) any applicable compensating controls;

(iii) the corrective action proposed; and

(iv) the expected timeframe for you to correct the Security Vulnerability; and

(b) you must complete our Third Party Information Security Assessment questionnaire and promptly respond to all consequential questions we may have.

8.2 If we consider that any report or answers provided in accordance with paragraph 8.1 is unsatisfactory we may, acting reasonably and at our cost, carry out or appoint a third party to carry out an independent security assessment of your security processes. This could include (and is not limited to) vulnerability assessments, penetration testing or controls testing of the Services, as a minimum the protective controls securing Vector Data and Vector Systems under this policy and any Agreement. Any such assessment will be subject to appropriate confidentiality obligations. You will provide all assistance and access to personnel and systems that we reasonably request.

8.3 If a security assessment reveals that your processes do not meet the minimum standards required by this policy or reveals significant deficiencies that result in a level of risk in relation to the Services that we consider unacceptable (acting reasonably), then you must promptly meet with us to discuss and agree appropriate corrective steps and apply those steps without delay.

9. Document control

Document author:	Monique Hogervorst (cyber security GRC manager)
Document owner:	Monique Hogervorst (cyber security GRC manager)
Document approved by:	Josh Reedy (acting GM cyber security)
Document published:	Public
Date of first issue:	1 September 2020
Previous version	March 2024
Last reviewed/reason:	March 2026 – regular review
Date for next review:	February 2028