Cyber Security Policy

1. Scope

1.1 This policy applies to all suppliers of software, services or other deliverables (Services) to Vector.

1.2 There are two parts to this policy:

(a) Part A applies to all suppliers; and

(b) Part B applies only to suppliers of Services that include the development of software, or the supply of software developed, by or on behalf of the supplier.

1.3 This policy applies in addition to any agreement (Agreement) between the supplier (you, your) and Vector. If there is an express 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. Any change will take effect when the updated policy is posted on Vector's website.

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.

Security Incident means the unauthorised access, use, alteration or destruction of any Vector Data or Vector Systems, or other compromise or reach 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 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 (wherever incorporated).

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 and, in relation to an Agreement, means the Vector Group company that is a party to that Agreement.

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.

Part A

2. Principles

2.1 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.

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. When that Agreement ends you must securely delete or destroy (or, if required by the Agreement, return) all Vector Data, except to the extent that you need the Vector

Data to perform obligations owed to us under another Agreement or to meet any regulatory obligations.

3.2 Where Vector Data includes personal information (as defined in the Privacy Act 1993 or any successor legislation), you must hold and process that personal information in accordance with our obligations under the Privacy Act 1993 or any successor legislation and our privacy policy, available at https://www.vector.co.nz/privacy-policy.

4. Security Requirements

4.1 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. This requirement applies whether the Services are provided directly by you or a third party and where the Services use an on-premise or cloud-based solution.

4.2 Without limiting your obligations under clause 4.1 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) comply with our password standard that:

(i.) requires passwords to be a minimum of twelve and a maximum of sixty-four characters in length;

(ii.) requires passwords to be changed every six months or immediately following a breach/specific threat;

(iii.) requires new passwords to be screened against lists of commonly used or known compromised passwords;

(iv.) requires new passwords to not be based on a previous password (a new password is required each time it is changed); and

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

(c) additional to the above, implement multi-factor authentication for all administrative accounts.

(d) 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;

(e) 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;

(f) 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;

(g) 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;

(h) regularly monitor the security of any network, infrastructure and systems that you use to provide Services to us and, at our request or when a significant incident occurs that could impact the Services, promptly report to us on any events that you detect and associated corrective actions;

(i) 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

(j) 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.

4.3 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 the integrity of Vector, you must:

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

(b) promptly provide all information we reasonably request in relation to the incident, its manner of introduction and the impact that the incident has had or 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 individuals involved in any aspect of the incident handling, 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.

4.4 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).

4.5 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 first notify us and, unless you have our prior written consent, you must only disclose the minimum required by law.

5. Information Security Audit

5.1 If you generate, collect, process, hold, store or transmit Vector Data or have access to any Vector Systems we may request that you:

(a) provide a written report summarising the result of any security assessment which is relevant to the Services and any risks identified during the security assessment, including:

(i.) a detailed description of any identified actual or potential Security Vulnerability;

(ii.) any applicable compensating controls;

(iii.) the corrective action proposed for any identified Security Vulnerability; and

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

(b) provide a complete copy of the full security assessment report; and/or

(c) engage, at our cost, a reputable independent third party to undertake an ISAE (NZ) 3402 (or equivalent) audit covering the security controls relevant to the Services and provide the auditor's report to us.

5.2 If we consider that any report provided in accordance with paragraph 5.1 is unsatisfactory we may, acting reasonably and at our cost, carry out ourselves or appoint a third party to carry out an independent security assessment of your security processes, including a vulnerability assessment, penetration testing or controls testing of the Services, and protection of Vector Data and Vector Systems under this policy and any Agreement, to identify potential Security Vulnerabilities. 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.

5.3 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.

Part B

6. Malicious Code and Security Vulnerabilities

6.1 You must take all precautions in accordance with Good Practice necessary to prevent the introduction of Malicious Code and Security Vulnerabilities to, or that impact on, the Services, Vector Data or Vector Systems, including:

(a) using best endeavours to ensure that, when you provide us with a Service, 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).

6.2 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.

7. Testing

7.1 Before providing any Service 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 Service (including any software provided as part of that Service):

(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.

7.2 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 the Vector Group in relation to that failure, including for eliminating or reversing any adverse effects of any destructive element.

8. Document control

Document author:	Katja Feldtmann
Document owner:	Katja Feldtmann
Document approved by:	Aaron McKeown
Document published:	Public
Date of issue:	1 September 2020
Last reviewed/reason:	September 2020 – Major revision and update to new corporate design
Date for next review:	September 2022