# Acceptable Use Policy

Version 1.0, last modified on 4 July 2017

## 1. Application

1.1. This Acceptable Use Policy (**“AUP”**) must be read in conjunction with any agreement into which it is incorporated by reference (**“Incorporating Agreement”**), including any agreement you have entered into with the Cloud Provider for services that are provided using the Cloud Provider's Network.

1.2. If there is conflict between this AUP and the Incorporating Agreement, the Incorporating Agreement will prevail.

1.3. This AUP applies where the Cloud Provider has provided you or any third party authorised by you with a connection to the Cloud Provider’s Network. It applies to any and all cloud services provided by the Cloud Provider to you or any third party authorised by you and to any third party authorised by the Cloud Provider including any customer, client, user, developer, employee, contractor, consultant, end user, partner, reseller, supplier or provider.

1.4. You acknowledge that this AUP may be amended from time to time by the Cloud Provider. When this occurs, an email notification will be sent.

1.5. By using or accessing the cloud services after this AUP has been amended you are deemed to have accepted and agreed to that amendment as legally binding on you and any third party authorised by you.

1.6. If any part of this AUP is held by any court or administrative body of competent jurisdiction to be unlawful, void or unenforceable, such determination will not impair the validity and enforceability of the remaining parts of this AUP.

1.7. In this AUP, unless the context otherwise requires:

1.7.1. **“Cloud Provider”** means the legal entity that provides the cloud services to you under the Incorporating Agreement.

1.7.2. **“Cloud Provider’s Network”** means any security management, backup, storage, monitoring system, account, network, network access, host, server, control device,

computer, communications system, software, data, computing device or other system provided by the Cloud Provider.

1.7.3. **“Third Party’s Network”** means any security management, backup, storage, monitoring system, account, network, network access, host, server, control device, computer, communications system, software, data, computing device or other system provided by a third party.

1.7.4. **“Your Network”** means any security management, backup, storage, monitoring system, account, network, network access, host, server, control device, computer, communications system, software, data, computing device or other system provided by you or a third party authorised by you.

## 2. Your Responsibilities

2.1. You acknowledge and accept sole responsibility and liability for any acts or omissions by you or any third party authorised by you to connect to the Cloud Provider’s Network.

2.2. You accept sole responsibility and liability for any and all disclosures or otherwise breaches of the confidentiality of your account log in details, including your user name, password, passphrase, PIN or security questions and answers.

## 3. Lawful Use

3.1. You acknowledge and agree that you and any third party authorised by you shall take reasonable steps to ensure and maintain the security of Your Network and to prevent activities that may compromise the security of the Cloud Provider's Network and to take any and all reasonable precautions to protect the Cloud Provider's Network from interference.

3.2. You agree to use the Cloud Provider's Network in a responsible manner, including:

3.2.1. To only connect to, access, use, make provision of, consume or otherwise make use of the Cloud Provider's Network for lawful purposes and that you are solely responsible for ensuring that your use or otherwise of the Cloud Provider's Network complies with all applicable laws;

3.2.2. To only connect to, access, use, make provision of, consume or otherwise make use of the Cloud Provider's Network for

the purpose for which it was intended by the Cloud Provider;

3.2.3. To follow any and all reasonable requests, instructions or directions in connection with any and all services provided over the Cloud Provider's Network as requested, instructed or directed by the Cloud Provider;

3.2.4. To protect your access or login details and to only provide them to any third party authorised by you to access the Cloud Provider's Network in accordance with any agreement you have with the Cloud Provider.

## 4. Prohibited Activities

4.1. You acknowledge and agree that you and any third party authorised by you shall not use or attempt to use the Cloud Provider's Network to engage directly or indirectly in activities that may:

4.1.1. Violate this AUP;

4.1.2. Violate any of the terms and conditions of any written agreement you may have with the Cloud Provider for any services provided to you by the Cloud Provider;

4.1.3. Infringe the rights of others or violate any applicable laws, regulations, treaties, government requirements, agreement, policy, practices, rule or other law or other regulatory or industry standard, code or practice;

4.1.4. Violate any agreement, policy, rule or other term or condition of any third party;

4.1.5. Violate any intellectual property right of any third party, including infringing or misappropriating any copyright, trademark, licence right, proprietary right or other legal protection of any intellectual property; or

4.1.6. Compromise the security of the Cloud Provider’s Network or a Third Party’s Network.

4.2. You agree not to directly, indirectly or attempt to guide, inform, assist, encourage, promote, foster, facilitate, engage in, use or instruct others to use the Cloud Provider's Network for the following prohibited activities:

4.2.1. Distributing, transmitting, re-transmitting or otherwise sending unwanted or unsolicited mass or bulk emails or other messages where:

4.2.1.1. there is no pre-existing relationship;

4.2.1.2. there is no accessible method for the recipient to unsubscribe;

4.2.1.3. the sender cannot be easily, readily or accurately identified in the header information or user identification;

4.2.1.4. a Third Party’s Network is used to relay mail without authorisation from that third party;

4.2.1.5. you use IP addresses that you do not have authorisation to use; or

4.2.1.6. the improper configuration of mail servers and/or FTP servers enables third parties to distribute, transmit, re-transmit or otherwise send unsolicited mass or bulk emails or other messages.

4.2.2. Collecting email addresses from the Internet by database scraping or database harvesting for the purpose of Spamming;

4.2.3. Falsifying, altering, amending, obscuring or otherwise disclosing any information (including packet headers, e-mail headers, email addresses or any other information about the sender of correspondence) in a manner that is misleading or has the potential to mislead;

4.2.4. Obtaining or using any information with the intention of impersonating a third party or assuming that party’s identity, without authorisation.

4.2.5. Introducing or using any malware, spamware, spyware, adware, viruses or any other malicious programmes, tools, software, code, file, script, command or otherwise that may damage, harm, deny, interfere with or expropriate any data from the Cloud Provider's Network or any Third Party’s Network;

4.2.6. Introducing or using any programmes, tools, software, code, file, script, command or otherwise that may damage or harm the Cloud Provider's Network or be used to engage in modem or system hi-jacking or otherwise;

4.2.7. Connecting to the Cloud Provider's Network by any means

other than by the supported interfaces provided by the Cloud Provider; or

4.2.8. Using any programmes, tools, software, code, file, script, command or otherwise that may circumvent any use limitations placed on any of the services provided by the Cloud Provider, including cloud services.

4.3. The Cloud Provider acknowledges that there may be a legitimate reason to carry out a prohibited activity to protect the anonymity of a user and that where a legitimate reason exists and the user has a reasonable expectation that their identity may be protected using anonymity, it is within the Cloud Provider’s sole discretion to determine, within reason, whether the prohibited activity is in breach of this AUP.

## 5. Security of Cloud Provider's Network

5.1. You agree not to directly, indirectly or attempt to guide, inform, assist, encourage, promote, foster, facilitate, engage in, use or instruct others to:

5.1.1. Probe, test, audit, scan or otherwise take any action aimed at monitoring the vulnerability or security of the Cloud Provider's Network, including scanning for open relays;

5.1.2. Hack, attack, gain access to, disable, disrupt, interfere with, compromise, breach or circumvent the security of the Cloud Provider's Network or any account associated on the Cloud Provider's Network, or cracking any authentication, encryption, password, passphrase, PIN or other security measure taken by the Cloud Provider or any other third party without the prior written approval of the Cloud Provider;

5.1.3. Hack, attack, abuse, block, disable, deny, interfere with, intercept or otherwise disrupt any third party’s connection to the Cloud Provider's Network, without the prior written approval of the Cloud Provider;

5.1.4. Hack, attack, abuse, block, disable, deny, interfere with, intercept or otherwise disrupt any third party’s use and enjoyment of any services provided by the Cloud Provider, without the prior written approval of the Cloud Provider, including unnecessarily excessive traffic;

5.1.5. Initiate an attack from the Cloud Provider's Network to hack,

abuse, block, disable, deny, interfere with, intercept or otherwise disrupt any services provided by a third party; or

5.1.6. Avoid payment for cloud services or attempt to obtain cloud services after your account with the Cloud Provider has been suspended or terminated.

## 6. Material and Content to be Hosted

6.1. You acknowledge and agree that you shall be solely and fully responsible for the content of any material that you upload or copy to the Cloud Provider's Network.

6.2. You must not use the Cloud Provider's Network to upload, copy or download material that is illegal according to New Zealand law.

6.3. You agree that you or any third party authorised by you must not post, store, upload, download, create, or otherwise provide any material or content for the Cloud Provider to host that would result in a violation of this AUP or any applicable laws, regulations, government requirements, agreement, rule, policy, practices or other law or other regulatory or industry standard, code or practice.

6.4. You acknowledge and agree not to host, transmit, send, receive, publish or otherwise make available any material or content that infringes a third party’s intellectual property rights including music, videos, books or software.

## 7. Violations of AUP

7.1. You will be held solely responsible for any violations by you and any third party authorised by you of this AUP including any and all breaches of security that are under your control, or the control of any third party authorised by you.

7.2. While the Cloud Provider has no obligation to monitor the Cloud Provider's Network for violations of this AUP, the Cloud Provider reserves the right to monitor the Cloud Provider's Network for violations of this AUP and reserves the right to investigate any and all suspected, alleged or otherwise violations of this AUP and to co-operate with government, law enforcement agencies, the courts, regulators or any other third parties, including any Internet Service Provider or telecommunications provider investigating an activity which is suspected of being, alleged to be or is deemed by the Cloud Provider to be a violation of this AUP.

7.3. Where an investigation is being undertaken into an activity on the Cloud Provider’s Network and the Cloud Provider is legally required

to disclose any information, material or otherwise, it will do so.

7.4. Insofar as is reasonably possible, the Cloud Provider will use reasonable endeavours to notify you in advance of any disclosure of information, material or otherwise, unless notification is legally prohibited.

7.5. The Cloud Provider disclaims all liability for any and all actions taken by the Cloud Provider in response to any suspected, alleged or otherwise violation of this AUP.

7.6. The Cloud Provider reserves the right to publish, disclose or otherwise provide information in accordance with the Privacy Act 1993 that relates directly or indirectly to any and all violations of this AUP to any third party that the Cloud Provider deems appropriate.

## 8. Reporting of Violations

8.1. If you become aware of any actual, alleged, suspected, prospective or future violation of this AUP, you must report that violation to the Cloud Provider immediately.

8.2. Any report, complaint or notification shall provide as much detail or information about the violation as possible to assist with any investigation.

8.3. Where the Cloud Provider has been notified by a third party of a violation of this AUP by you, or any third party authorised by you, the Cloud Provider reserves the right not to disclose any information to you until such time as the Cloud Provider in its sole discretion deems it appropriate.

## 9. Consequences of Violations

9.1. Any violation of this AUP will be deemed to be a material breach of any agreement you have entered into with the Cloud Provider and the Cloud Provider may take any action it deems fit in accordance with any of the provisions contained in any agreement you may have with the Cloud Provider.

9.2. Any violation of this AUP is strictly prohibited, and at any time the Cloud Provider in its sole discretion may immediately and without notice take any action it deems fit, including without limitation any or all of the following:

9.2.1. Require you to take prompt or immediate corrective steps to remedy the violation;

9.2.2. Require you to take steps to prevent a future or prospective violation;

9.2.3. Issue you a warning or notice of violation;

9.2.4. Prohibit access to the material or content that violates this AUP, including blocking or filtering;

9.2.5. Take any steps it deems fit to prevent, stop or remedy the violation;

9.2.6. Charge you with any and all direct or indirect costs incurred for the Cloud Provider to address the violation;

9.2.7. Suspend the services, in whole or in part;

9.2.8. Terminate the services, in whole or in part;

9.2.9. Initiate legal proceedings against you or any other third party seeking any legal remedies available to it, including any damages, costs, expenses or other costs incurred directly or indirectly as a result of a violation of this AUP;

9.2.10. Engage in disclosure to government, courts or any law enforcement agency which may result in criminal charges, prosecution, liability, sanction or other censure;

9.2.11. Engage in disclosure to a regulator or any other investigating body, including any Internet Service Provider or telecommunications provider, which may result in civil proceedings, liability, disciplinary action, sanction or other censure;

9.2.12. Co-operate with government, law enforcement agencies, courts, regulators, or any other third party, including any Internet Service Provider or telecommunications provider investigating an activity which is suspected of being, alleged to be or is deemed by the Cloud Provider to be a violation of this AUP;

9.2.13. Any other action in accordance with any agreement you may have with the Cloud Provider; or

9.2.14. Any other action that the Cloud Provider in its sole discretion deems appropriate.