Service Terms

Version 4.7, last modified 06 October 2020.

1. Application

1.1. These Service Terms (**"Service Terms"**) must be read in conjunction with any agreement into which they are incorporated (**"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 any conflict between these Service Terms and the Incorporating Agreement, the Incorporating Agreement will prevail.

1.3. You acknowledge that these Service Terms may be amended from time to time by the Cloud Provider. When this occurs, an email notification will be sent to you.

1.4. By using or accessing the Cloud Services after these Service Terms have been amended, modified, varied or supplemented, you are deemed to have accepted and agreed to that amendment as legally binding on you and any third party authorised by you.

2. Definitions

2.1. Unless otherwise expressly defined within these Service Terms all capitalised terms used within these Service Terms are deemed to have the meaning set out in the Incorporating Agreement.

2.2. In these Service Terms, unless the context otherwise requires:

> **"Alpha"** means a service or software that is under active development and in stages of testing. Its purpose is to establish a feedback loop, allowing customers to influence its development and direction. Backward incompatible changes may be introduced to the service or its APIs. Services or software classified as Alpha are not recommended for production workloads.
>
> **"Beta"** means a service or software that is undergoing testing and has no Service Level Objectives associated with it yet. It is expected

to be used under real conditions, but may contain known bugs or be changed before the final version is released. Cloud Customers are required to use their own judgement and discretion to assess if the Beta version is suitable for the purposes they have in mind.

"Cloud Customer" means:

(a) you on an individual basis, or the company, business, organisation, association or other entity that you (or any third party authorised by you) provided in the application to become a Cloud Customer;

(b) where that application to become a Cloud Customer has been submitted to the Cloud Provider; and

(c) where the Cloud Provider has accepted that application;

"Cloud Data" means any information, data, files, documents, objects, software, applications, and any other information that the Cloud Customer uploads into the cloud in accordance with the provision of Cloud Services to that Cloud Customer;

"Cloud Provider" means the legal entity which sells the Cloud Services to you under the Incorporating Agreement;

"Confidential Information" means all information provided to the Cloud Provider by the Cloud Customer or any third party authorised by the Cloud Customer, including any Cloud Data, any information provided in the Application Form and all materials, documentation and records provided to the Cloud Provider or created by the Cloud Provider that directly relate to the Cloud Customer, other than information which:

(a) is or becomes publicly available through no fault of the Cloud Provider; or

(b) is independently acquired or developed by the Cloud Provider without breaching any of its obligations under law, and without the benefit or use of any Confidential Information disclosed by the Cloud Customer; or

(c) is lawfully acquired by the Cloud Provider from a third party,

provided that such information is not obtained as a result of a breach by that third party of any confidentiality obligations owing to the Cloud Customer;

“Downtime Period” means the time in minutes that a Cloud Service was affected by an Unscheduled Outage;

“Emergency Outage” means any disruption or interruption to the provision of Cloud Services that was planned for the Cloud Provider to resolve any critical, necessary or significant matters including faults, failures, security threats or breaches, and where it is necessary to resolve that matter urgently, imminently, or immediately with no notice or with minimal notice;

“Monthly Uptime Percentage” means the total number of minutes in a month, minus the Downtime Periods in a month, divided by the total number of minutes in a month;

“SLA Credit” means the financial amount that the Cloud Provider will credit to the Cloud Customer’s account if the Cloud Provider fails to meet Service Level Objectives;

“Service Level Objective (SLO)” means the target service levels defined by the Cloud Provider in respect of a Cloud Service, as set out in these Service Terms;

“Scheduled Maintenance Window” means the planned period of time allocated by the Cloud Provider to carry out maintenance on the cloud or any of the Cloud Services (where there is a risk that the maintenance may directly or indirectly result in an Unscheduled Outage);

“Scheduled Outage” means any disruption or interruption to the provision of Cloud Services that was scheduled in advance of its occurrence;

“Technical Documentation” means the documentation for the Cloud Services made available via the Dashboard or the Cloud Provider’s website; and

“Unscheduled Outage” means any disruption or interruption to the provision of Cloud Services that was not scheduled in advance of its

occurrence.

3. Cloud Services

3.1. Cloud Customers use a control plane to provision and manage Cloud Services (**"Control Plane"**). The following Cloud Services are considered to be part of the Control Plane:

3.1.1. **"API"** - an application programming interface used by software, services, applications or other programs to interact with the Cloud Services; and

3.1.2. **"Dashboard"** - a visual web interface used by people to interact with the Cloud Services.

3.2. In addition to the above, the Cloud Provider offers the following Cloud Services in whole or in part:

3.2.1. **"Block Storage"** – a service that provides virtual block volumes that can be attached to compute instances for data storage;

3.2.2. **"Cloud Orchestration"** – a service that allows applications or infrastructure to be automatically provisioned and configured on the cloud, based on templates;

3.2.3. **"Compute Service"** – a service that enables the Cloud Customer to provision and manage compute instances (also known as virtual machines);

3.2.4. **"Direct Connection"** – a service that allows customers to establish a dedicated network connection to the cloud for consistent network performance, increased throughput and increased security;

3.2.5. **"Identity & Access Management Service"** – a service that allows customers to control and delegate access to its account and cloud services to employees or third parties;

3.2.6. **"Image Service"** – a service that enables the Cloud Customer to create or upload disk images and metadata definitions that can be used to boot compute instances or block volumes;

3.2.7. **"Network Service"** – a service that connects compute instances to

each other and enables them to gain access to the Internet;

3.2.8. **"Kubernetes Service"** – a platform service that makes it easy to deploy, manage, and scale Kubernetes clusters to run containerised applications;

3.2.9. **"Load Balancer Service"** – a service distributes network traffic to compute instances or applications hosted in the cloud, allowing them to be scaled or to improve their fault tolerance;

3.2.10. **"Object Storage"** – a service that enables the Cloud Customer to store and retrieve any type of data on the cloud;

3.2.11. **"VPN Service"** – virtual private network as a service: a service that enables a network that exists outside the cloud to be security extended into the cloud; and

3.2.12. **"Premium Support"** – a service that enables the Cloud Customer to access increased support levels from the Cloud Provider, as described in the Pricing Schedule.

4. General Terms and Conditions for all Cloud Services

4.1. With the exception of clause 5 (Specific Services), the following terms of service apply to all offerings of Cloud Services:

4.1.1. The Cloud Customer acknowledges and agrees that the Cloud Provider is solely responsible for, at the Cloud Provider's sole discretion, implementing any up-to-date patches and the latest security, operating system and software updates and upgrades to the Cloud Services and related infrastructure;

4.1.2. In addition to the responsibilities, duties and obligations set out in the Incorporating Agreement, the Cloud Customer acknowledges and accepts that the Cloud Customer is solely responsible for:

4.1.2.1. Complying with the current Technical Documentation, such as the latest API specification, for the Cloud Services;

4.1.2.2. Uploading Cloud Data to the cloud and maintaining a copy of the Cloud Data external to the cloud; and

4.1.2.3. Maintaining regular backups of the Cloud Data and for the security and protection of those backups;

4.1.3. The Cloud Provider will undertake periodic maintenance on the Cloud Services with a view to ensuring their optimal performance. In most cases maintenance will have limited or no negative impact on the service levels;

4.1.4. Where planned maintenance is expected to affect the service levels, the Cloud Provider will use commercially reasonable efforts to provide the Cloud Customer with at least ten (10) Business Days' notice of the outage;

4.1.5. The Cloud Provider reserves the right to perform emergency maintenance at any time to resolve any critical, necessary or significant matters such as faults, failures or security threats. The Cloud Provider will use commercially reasonable efforts to notify the Cloud Customer in advance of any Emergency Outage where it is practical to do so; and

4.1.6. Where there is an Unscheduled Outage, the Cloud Provider will use commercially reasonable efforts to restore the Cloud Services as soon as possible.

5. Control Plane Specific Terms

5.1. The following terms of service apply only to the **Control Plane**:

5.1.1. The Cloud Customer acknowledges that, in general, outages of the Control Plane do not affect the availability of other Cloud Services;

5.1.2. The Cloud Customer acknowledges that the Control Plane may not be available for use from time to time for reasons including maintenance, upgrade, repair, fault or failure; and

5.1.3. The Cloud Provider will take reasonable steps to minimise any disruptions or interruptions to use of the Control Plane.

6. Block Storage Specific Terms

6.1. The following terms of service apply only to the **Block Storage Service**:

6.1.1. With the exception Wellington region, Cloud Data stored in the Block Storage Service is encrypted at rest and the Cloud Provider holds the encryption keys;

6.1.2. With the exception of Scheduled Outages, the Cloud Provider will use reasonable efforts to provide a Monthly Uptime Percentage of 99.95% for the storage types with three replicas provided by the Block Storage Service; and

6.1.3. Where the Cloud Provider has failed to meet the Service Level Objective for the Block Storage Service defined in clause 6.1.2, the Cloud Customer will be entitled to SLA Credits for the affected block storage volumes only, in accordance with the table below:

Monthly Uptime Percentage	**SLA Credit**
Less than 99.95%, but greater than 99.00%	20%
Less than 99.00%, but greater than 95.00%	30%
Less than 95%	50%

7. Compute Service Specific Terms

7.1. The following terms of service apply only to the **Compute Service**:

7.1.1. The Cloud Customer is responsible for:

7.1.1.1. The configuration of the Cloud Customer's compute instances, including any configuration that would enable it to start up automatically where there is a server failure; and

7.1.1.2. for managing the compute instance and any and all matters relating to the operating system and any other software within the compute instance;

7.1.2. The Cloud Customer acknowledges and accepts that the Cloud Provider takes no responsibility and cannot be held liable for any loss, misuse or unauthorised access, modification, or disclosure of

Cloud Data that may occur directly or indirectly from the configuration of a compute instance, or from any server failure or from restarting compute instances;

7.1.3. With the exception of Scheduled Outages, the Cloud Provider will use reasonable efforts to provide a Monthly Uptime Percentage of 99.95% for the Compute Service, as measured by the Cloud Provider's monitoring service at the hypervisor level; and

7.1.4. Where the Cloud Provider has failed to meet the Service Level Objective for the Compute Service defined in clause 7.1.3, the Cloud Customer will be entitled to SLA Credits for the affected compute instances only, in accordance with the table below:

Monthly Uptime Percentage	**SLA Credit**
Less than 99.95%, but greater than 99.00%	20%
Less than 99.00%, but greater than 95.00%	30%
Less than 95%	50%

8. Direct Connect Service Specific Terms

8.1. The following terms of service apply only to the **Direct Connect Service:**

8.1.1. The Cloud Customer acknowledges and accepts that Direct Connect Service is provided as a Beta service.

9. Identity & Access Management Service Specific Terms

9.1. The following terms of service apply only to the **Identity and Access Management Service**:

9.1.1. The Identity and Access Management Service allows the Cloud Customer to control and delegate access to its account to its employees or third parties; and

9.1.2. Identity credentials must not be shared with other people using

insecure channels, such as email, or stored in an unsafe way, such as in public repositories.

10. Image Service Specific Terms

10.1. The following terms of service apply only to the **Image Service**:

10.1.1. The Cloud Customer acknowledges and accepts the Cloud Customer is solely responsible for:

10.1.1.1. Uploading media or machine images to the Image Service (with the exception of media or machine images uploaded by the Cloud Provider or its duly authorised agent);

10.1.1.2. Maintaining the security and protection of the images and controlling access to the images; and

10.1.1.3. Determining whether the image is fit for purpose and suitable for the Cloud Customer's use.

10.1.2. The Cloud Customer acknowledges that by sharing an image, the data contained within that image will be available to view, use, download and otherwise by other Cloud Customers and that the Cloud Provider takes no responsibility for any loss of privacy or breach of confidentially as a direct or indirect result of the sharing of an image.

11. Kubernetes Service Specific Terms

11.1. The following terms of service apply only to the **Kubernetes Service:**

11.1.1. The Cloud Provider makes well tested and certified cluster templates available to customers to deploy, configure and upgrade Kubernetes clusters. When customers use these templates, without modification, the Cloud Provider is responsible for:

11.1.1.1. Providing support for three major versions of Kubernetes, allowing customers at least six months time to plan and perform (major) upgrades;

11.1.1.2. Providing security updates for the base operating system, the Docker Engine and/or Kubernetes, in the form of new

template versions;

11.1.1.3. Applying critical security updates to the base operating system, Docker Engine and/or Kubernetes, on behalf of customers that have not opted out of automated security updates. These automatic updates will be restricted to patch versions only (for example Kubernetes version 1.18.1 to 1.18.2);

11.1.1.4. Notifying customers about known critical security vulnerabilities and updates;

11.1.1.5. Monitoring the availability of the Kubernetes clusters and resolving incidents impacting the control plane, master or worker nodes.

11.1.2. Cloud Customers are responsible for:

11.1.2.1. The software, configuration and data in containers deployed to Kubernetes, including security updates and upgrades of these applications;

11.1.2.2. Any configuration, metadata or secrets stored in Kubernetes;

11.1.2.3. Performing major or minor upgrades, at a time appropriate for its business, using the provided upgrade API.

11.1.3. Cloud Customers are recommended to:

11.1.3.1. Use highly available clusters (the production cluster template with at least three master nodes) for production workloads;

11.1.3.2. Keep their Kubernetes clusters private (APIs and cluster nodes not visible to the internet) where possible. If access is required from additional hosts or subnets, restrict API and node access to specific CIDRs;

11.1.3.3. Not store any data on the ephemeral container file system. Application data should be stored on persistent volumes or external services like object storage or database;

11.1.3.4. Only deploy container images that have been inspected and are trusted by the customer. Update container images and deployments frequently, so that the latest security updates are applied to them;

11.1.3.5. Not make changes to the pre-configured software deployed by the Cloud Provider to the "kube-system" namespace. If modified, the customer assumes responsibility for their ongoing maintenance and exempt the Cloud Provider from incidents caused by them.

11.1.4. The Cloud Customer acknowledges and accepts that the Cloud Provider takes no responsibility and cannot be held liable for any loss, misuse or unauthorised access, modification, or disclosure of Cloud Data that may occur directly or indirectly as a result of the software or configuration of its containers or Kubernetes resources (such as Pods, ReplicaSets, Deployments).

11.1.5. With the exception of Scheduled Outages, the Cloud Provider will use reasonable efforts to provide a Monthly Uptime Percentage of 99.95% for the Kubernetes APIs (control plane) of highly available clusters (three or more master nodes). The availability of individual worker nodes is covered by the Compute Service SLA.

12. Load Balancer Service Specific Terms

12.1. The following terms of service apply only to the **Load Balancer Service:**

12.1.1. The Cloud Provider is responsible for:

12.1.1.1. Applying security updates to the base operating system and/or software that provides the load balancing service;

12.1.1.2. Notifying customers of any known critical security vulnerabilities that would fail to enforce any configuration that the customer has specified;

12.1.1.3. Monitoring the availability of the load balancing service, and resolving incidents that impact the load balancing service, excluding health monitoring which the load balancer uses to determine if the customer's configured targets are available

12.1.1.4. Ensuring that traffic that traverses the load balancer is not modified unless the Cloud Customer has explicitly configured the load balancer to do so;

12.1.1.5. Protecting the load balancer operating system from unauthorised access.

12.1.2. Cloud Customers are responsible for:

12.1.2.1. Monitoring of the availability of targets of the load balancer, and resolving any incidents which affect the load balancer's decision to use or not use a specific target;

12.1.2.2. Configuration of health checks in the load balancer to inform the load balancer of what targets are able to be used;

12.1.2.3. Defining the policy the load balancer will apply to traffic directed towards it, including the security implications of the load balancer passing traffic towards any target

12.1.2.4. Defining any restrictions on address ranges which may direct traffic towards the load balancer;

12.1.2.5. Configuration of any security groups, firewalls, or other access controls in front or implemented by a target that allows the load balancer to direct traffic to the target, including where this is implemented by another Service provided by the Cloud Provider;

12.1.2.6. Ensuring the security of any system that is a target of the load balancer;

12.1.2.7. Determining if the load balancer shall have a public IP address associated with it, for reception of traffic from the public Internet;

12.1.2.8. Any and all methods needed to associate the IP address(es) of a load balancer with a service, such as DNS records or software configuration.

12.1.3. Cloud Customers are recommended to:

12.1.3.1. Maintain suitable logs of access to targets, where possible using additional information inserted by the load balancer on the original origin of the traffic;

12.1.3.2. Avoid attaching public IP addresses to load balancers that are intended to be private;

12.1.3.3. Limit the ports that a load balancer is configured to accept traffic on to only those required by their application(s);

12.1.3.4. Configure the load balancer to reject connections from IP addresses outside specific address ranges;

12.1.3.5. Place additional layers of protection in front of any load balancer, such as DDoS protection, Web Application Firewalls, or Identity Management, to protect their application.

12.1.4. The Cloud Customer acknowledges and accepts that the Cloud Provider takes no responsibility and cannot be held liable for any loss, misuse or unauthorized access, modification, or disclosure of Cloud Data that may occur directly or indirectly as a result of the configuration of the load balancer as specified by the customer.

12.1.5. The Cloud Provider will use reasonable efforts to maintain a Month Uptime Percentage of 99.95% for the load balancing service with the following exceptions:

12.1.5.1. Scheduled downtime of the service;

12.1.5.2. The service is deemed to be available even if all health checks configured by the Cloud Customer fail, provided the checks configured by the customer are being executed by the load balancing service exactly as specified by the Cloud Customer to the load balancing service.

12.1.6. Where the Cloud Provider has failed to meet the Service Level Objective for the Compute Service defined in clause 12.1.5, the Cloud Customer will be entitled to SLA Credits for the affected load balancer instances only, in accordance with the table below:

Monthly Uptime Percentage	**SLA Credit**

Less than 99.95%, but greater than 99.00%	20%
Less than 99.00%, but greater than 95.00%	30%
Less than 95%	50%

13. Object Storage Specific Terms

13.1. The following terms of service apply only to the **Object Storage Service**:

13.1.1. Cloud Data stored in the Object Storage Service is encrypted at rest and the Cloud Provider holds the encryption keys.

13.1.2. By default, three replicas of the Cloud Data are preserved. The replicas are initially stored in the same Region and then replicated asynchronously to two other Regions after some time.

13.1.2.1. To reduce storage costs, Cloud Customers can opt for reduced data durability. Cloud Customers should make this choice understanding that its risks and implications are acceptable for their business.

13.1.3. With the exception of Scheduled Outages, the Cloud Provider will use reasonable efforts to provide a Monthly Uptime Percentage of 99.9% for the Object Storage Service; and

13.1.4. Where the Cloud Provider has failed to meet the Service Level Objective for the Object Storage Service defined in clause 13.1.3, the Cloud Customer will be entitled to SLA Credits for the affected objects only, in accordance with the table below:

Monthly Uptime Percentage	**Service Credit Percentage**
Less than 99.9% but greater than or equal to 99%	10%
Less than 99.0% but greater	25%

Monthly Uptime Percentage	Service Credit Percentage
than or equal to 95%	
Less than 95%	100%

14. VPN Specific Terms

14.1. The following terms of service apply only to the **VPN Service:**

14.1.1. The Cloud Customer acknowledges and accepts that VPN Service is provided as a Beta service.

15. Credit Request and Claim Procedure

15.1. Subject to this clause 15, where the Cloud Provider has not met the Service Level Objective for a Cloud Service in a given month, the Cloud Customer will be entitled to SLA credits.

15.2. The Cloud Customer will not entitled to SLA credits if:

15.2.1. The Cloud Customer is in breach of the Cloud Agreement, including payment obligations;

15.2.2. The service failure was caused by misuse of the Cloud Service by the Cloud Customer;

15.2.3. The service failure was caused by factors outside of the Cloud Provider's reasonable control, including any force majeure event, or Internet access or related problem; or

15.2.4. The event occurred during scheduled maintenance.

15.3. To receive SLA credits, the Cloud Customer must submit a claim to its account manager within thirty (30) days of the Cloud Provider's failure to meet the relevant Service Level Objective. The request must include:

15.3.1. The dates and times of each Unscheduled Outage;

15.3.2. The IDs of the affected Cloud Services; and

15.3.3. Any information or error logs that that support the claim.

15.4. A failure to make a timely claim for SLA credits or to provide any other supporting information reasonably requested by the Cloud Provider may disqualify the Cloud Customer from receiving SLA credits.

15.5. The Cloud Provider will credit SLA credits to the Cloud Customer's account upon confirming that the relevant Service Level Objective has not been met.

15.6. SLA credits may only be used against future invoices for Cloud Services and will expire after ninety (90) days from the date on which they are issued. The Cloud Customer is not entitled to any refund or payment by the Cloud Provider in such circumstances.

16. Violation of Service Terms

16.1. Any violation of these Service Terms will be deemed to be a material breach of the Cloud Agreement and may result in suspension or termination in accordance with the Incorporating Agreement.

17. Confidentiality

17.1. The Could Provider recognises that the Confidential Information is confidential and agrees that:

17.1.1. The Cloud Data is designated as Confidential Information; and

17.1.2. The Cloud Data is the property of the Cloud Customer.

17.2. Except to the extent permitted under these Service Terms or the Incorporating Agreement, the Cloud Customer agrees to disclose Confidential Information to the Cloud Provider and the Cloud Provider agrees to keep confidential all Confidential Information and to use the Confidential Information solely for the purposes of the Cloud Agreement and not for any other purpose.

17.3. The Cloud Customer agrees not to issue to the media any press release or announcement relating to the cloud or the Cloud Services without Cloud Provider's prior written consent.

18. Data Collection

18.1. The Cloud Customer is solely responsible for uploading the Cloud Data into the cloud. The Cloud Customer agrees that any Cloud Data that has been

uploaded to the cloud under the Cloud Customer's account is deemed to have been provided to the Cloud Provider directly by the Cloud Customer.

18.2. The Cloud Customer recognises that, by uploading the Cloud Data to the cloud, the Cloud Provider shall store and have access to the Cloud Data on the cloud.

18.3. The Cloud Customer recognises that:

18.3.1. A function or activity of the Cloud Provider is to provide Cloud Services to its Cloud Customers;

18.3.2. The Cloud Data is collected for a lawful purpose connected with that function or activity; and

18.3.3. That the collection of the Cloud Data is necessary for that purpose.

18.4. The Cloud Customer acknowledges and accepts that the Cloud Provider will store the Cloud Data in accordance with Clause 19.1, solely as the Cloud Customer's agent on one or more of the Cloud Provider's servers at one or more of its cloud regions located in New Zealand and the Cloud Customer agrees that the Cloud Provider is deemed to be the intended recipient of the Cloud Data.

19. Data Protection

19.1. The Cloud Customer acknowledges and accepts that:

19.1.1. The Cloud Provider is responsible for the design, architecture, implementation, infrastructure and operation of the cloud and the Cloud Services; and

19.1.2. The Cloud Customer is responsible for the Cloud Customer's network and its configuration, configuring the Cloud Services, managing the Cloud Customer's access, use, provision, maintenance and consumption of Cloud Services and for any software, applications, systems or other programs that the Cloud Customer has installed or configured to operate within the cloud.

19.2. In accordance with Clause 19.1.1, the Cloud Provider is responsible for the security and protection of the cloud and will put in place such safeguards as is reasonable in the circumstances for the Cloud Provider to take against

unauthorised access, use, modification, disclosure, loss or other misuse of Cloud Data.

19.3. In accordance with Clause 19.1.2, the Cloud Customer is responsible for the security and protection thereof and will put in place such safeguards as is reasonable in the circumstances for the Cloud Customer to take against unauthorised access, use, modification, disclosure, loss or other misuse of Cloud Data.

20. Use of Data

20.1. From the Commencement Date and thereafter, the Cloud Provider may use any Confidential Information for any of the purposes set out in the Incorporating Agreement or any other written agreement between the Cloud Provider and the Cloud Customer, and to otherwise exercise the Cloud Provider's rights and fulfil its duties and obligations under the Incorporating Agreement and all things incidental to the Incorporating Agreement.

20.2. The Cloud Provider will not at any time use the Cloud Data to target or serve advertisements.

20.3. The Cloud Provider will only use the Cloud Data for the purpose that it was obtained and will not use the Cloud Data for any other purpose unless the Cloud Provider believes on reasonable grounds that the purpose for which the Cloud Data is used is directly related to the purpose for which the information was obtained, or for any other lawful purpose in accordance with the Privacy Act 1993.

21. Disclosure of Data

21.1. The Cloud Provider may allow access to or disclose Confidential Information to a third party including its duly authorised agents where:

21.1.1. such disclosure is necessary for the provision of the Cloud Services or occurs as part of a routine professional security audit by that third party;

21.1.2. The Cloud Provider has informed that third party of the confidential nature of the Confidential Information and its obligations under the Cloud Agreement; and

21.1.3. That third party has signed a non-disclosure agreement or an

agreement containing a non-disclosure provision.

21.2. With the exception of clause 21.1 and 21.3, the Cloud Provider shall not disclose Confidential Information to any other third party unless:

21.2.1. The Cloud Provider believes on reasonable grounds that the disclosure of the Confidential Information is one of the purposes in connection with which the Confidential Information was obtained or is directly related to the purposes in connection with which the Confidential Information was obtained;

21.2.2. The Cloud Provider reasonably believes it is legally required to disclose the Confidential Information;

21.2.3. Disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences; or

21.2.4. For any other lawful purpose in accordance with the Privacy Act 1993.

21.3. Where government, regulators or law enforcement request the Cloud Provider to disclose Confidential Information, but where the Cloud Provider is not legally required to disclose that Confidential Information, the Cloud Provider will:

21.3.1. Notify the Cloud Customer of the request for disclosure, unless notification is legally prohibited;

21.3.2. Attempt to refer the request for disclosure to the Cloud Customer; and

21.3.3. Within reason, cooperate with the Cloud Customer's efforts to resist disclosure.

21.4. Where a third party requests that the Cloud Provider disclose Confidential Information, and where the Cloud Provider has reason to believe it is legally required to disclose that Confidential Information, the Cloud Provider will, where legally permitted, take such steps as are reasonable in the circumstances to notify the Cloud Customer of:

21.4.1. The fact that the disclosure is authorised or required under the law;

21.4.2. The particular law by or under which the disclosure is so authorised or required; and

21.4.3. The name and address of the third party to whom the disclosure is to be made.

21.5. The Cloud Customer acknowledges and accepts that the Cloud Provider takes no responsibility whatsoever for disclosure of Confidential Information by any third party or of breaches to the security of the cloud.

21.6. Where either party receives a request to extract Cloud Data from the cloud, the Cloud Customer is responsible for complying with a request for disclosure and extracting that Cloud Data, unless it is not legally permitted for the Cloud Customer to do so. This subclause 21.6 clause does not restrict the Cloud Provider.

22. Data Storage

22.1. The Cloud Provider shall not host the cloud in any place outside of New Zealand.

22.2. The Cloud Provider agrees:

22.2.1. To host the cloud within New Zealand at one or more datacentres;

22.2.2. That those datacentres have obtained reasonable security standards and that those security standards will be reasonably maintained;

22.2.3. That the Cloud Provider has taken commercially reasonable and appropriate technical and organisational measures to maintain the security of the cloud regions and datacentres; and

22.2.4. That the Cloud Provider's systems and procedures are industry standard or better.

22.3. The Cloud Provider or its duly authorised agent is responsible for the physical security of its cloud regions and will take such security safeguards as are reasonable in the circumstances to take against a breach of the physical security of its cloud regions.

22.4. The Cloud Customer acknowledges and accepts that the Cloud Data will transit through other jurisdictions any time the Cloud Data is accessed from outside of New Zealand and at times when the Cloud Data is accessed from inside New Zealand, due to the nature of Internet routing protocols.

22.5. The Cloud Provider takes no responsibility for data in transit, including any transit through other jurisdictions. The Cloud Provider recommends that the Cloud Customer encrypt data in transit in accordance with industry best practice.

22.6. The Cloud Customer accepts and agrees that it is solely responsible for any and all corrections to the Cloud Data.

23. Security Audits

23.1. The Cloud Provider may conduct periodic security audits of the cloud at the frequency and regularity that the Cloud Provider deems fit, including through employing an auditor or security specialist.

23.2. The Cloud Provider reserves the right to maintain the confidence of the full and complete audit report.

23.3. Where the Cloud Customer requests disclosure of and the Cloud Provider deems it appropriate, the Cloud Provider may disclose the audit certificate and summary of the audit report to the Cloud Customer. The Cloud Provider reserves the right not to disclose the full and complete audit report, the summary of the audit report, the audit certificate or any other information pertaining to the security audit.

24. Account Security

24.1. The Cloud Provider may provide the Cloud Customer with one or more logins to access the Cloud Customer's account, including the cloud management interface.

24.2. The Cloud Customer is solely responsible for maintaining security and protection of the Cloud Customer's logins, including controlling access and permissions.

24.3. The Cloud Customer accepts that the Cloud Provider is entitled to rely on the provision of the login, usernames, security password, passphrases or personal identification numbers as evidence of authority to access the Cloud

Customer's account and to legally bind the Customer.

24.4. The Cloud Customer takes full and complete responsibility for any and all use or misuse of the Cloud Services by the Cloud Customer or any third party accessing Cloud Services through the Cloud Customer's account, irrespective of whether authorised by the Cloud Customer and irrespective of whether there is evidence of authority to access the Cloud Customer's account.

25. Security: Breach Notification

25.1. If the Cloud Provider or its duly authorised agent becomes aware of, or has reason to suspect the existence of, any incident involving unauthorised access to or modification or any component of the Cloud Services, or Cloud Data stored in or transiting through the Cloud Services:

25.1.1. The Cloud Provider will promptly notify the affected Cloud Customer that a security breach has occurred, the type of security breach and the timing and duration of the security breach;

25.1.2. The Cloud Provider will take all commercially reasonable steps available to the Cloud Provider to ascertain the nature and causes of the incident and identify what Cloud Data was affected, and share with the affected Cloud Customer all results of those investigations;

25.1.3. The Cloud Provider will make reasonable efforts to co-operate with the affected Cloud Customer's own investigations, and provide reasonable assistance with the affected Cloud Customer's efforts to recover and secure Cloud Data that has been lost, corrupted, modified or misappropriated as a result of the incident; and

25.1.4. The Cloud Provider will such changes to the Cloud Services as may be reasonable and necessary to prevent similar occurrences in the future, and report to the affected Cloud Customer on the steps taken.

25.2. Where the Cloud Provider has reason to believe that a security breach has occurred or is at risk of occurring, the Cloud Provider has the right to disable, block or otherwise suspend services temporarily, in whole or in part, to any and all Cloud Customers affected or likely to be affected by that

security breach, resulting in an Emergency Outage until such time as the Cloud Provider has satisfied itself that the security breach has been resolved. The Cloud Provider will use commercially reasonable endeavours to resolve security breaches as swiftly as reasonably possible.