Service Terms

Version 5.2 – 1 February 2023

Table of contents

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 shall 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 with 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:

"**Agreed Service Level**" means the minimum service levels defined by the Cloud Provider in respect of a Cloud Service, as set out in these Service Terms;

"**Beta**" when applied to a service means that service incomplete or undergoing testing, and is subject to the terms of clause 4.10 and all sub-clauses within.

"**Cloud Customer**" means:

a. you on an individual basis, or the company, business, organisation, or

association or other entity that you (or a 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, or causes to be created or processed within 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;

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;

"**Generally Available**" when applied to a Cloud Service, means that service is available to all customers, has an Agreed Service Level and is considered by Catalyst Cloud to be appropriate for production workloads, and is subject to notification processes for changes to the Cloud Service;

"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;

"**Service Level Credit**" means the financial amount that the Cloud Provider will credit to the Cloud Customer's account if the Cloud Provider fails to meet an Agreed Service Level for a service;

"**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;

"**Technical Preview**" when applied to a service means that service is under active development, and subject to the terms of clause 4.11 and all sub-clauses within; 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 Customer uses a control plane to provision and manage Cloud Services ("**Control Plane**"). The following Cloud Services are considered to be part of the

Control Plane:

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

"**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:

"**Alarms**" – a service that will observe metrics generated by the platform for resources, and invoke another API to take action when metrics are outside customer-defined ranges;

"**Audit Log**" – a service that delivers records of activity and events for consumption by the Cloud Customer's monitoring systems;

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

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

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

"**Direct Connect**" – a service that allows a Cloud Customer to establish a dedicated, private, network connection to the cloud for consistent network performance, increased throughput, and increased security;

"**DNS Hosting Service**" – a service that allows a Cloud Customer to manage Domain Name System zones and records, with zones served by the Cloud Provider;

"**Identity and Access Management Service**" – a service that allows a Cloud Customer to control and delegate access to its account(s) and cloud services to other people, third parties, services or machines;

"**Image Service**" – a service that enables the Cloud Customer to create or upload copies of disks and metadata definitions that can be used to provision compute instances or to seed block volumes;

"**Ingress Protection**" – A service which limits traffic from the Internet from causing harm to customer and platform services that are exposed to the Internet;

"**Kubernetes Service**" – a service that enables the Cloud Customer to deploy, manage, and scale Kubernetes clusters to run containerised applications;

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

"**Managed Database Service**" – a service that enables the Cloud Customer to create one or more instances with a pre-installed database engine of their choice from the list of supported engines, with configuration defined by the Cloud Customer automatically applied;

"**Network Service**" – a service that enables the Cloud Customer to create and manage network constructs such as virtual networks, virtual routers, and network connections to cloud services and the Internet;

"**Object Storage**" – a service that enables the Cloud Customer to store and retrieve data in an unstructured manner, without operating servers, in a highly durable manner;

"**Premium Support**" – a service that enables the Cloud Customer to access support services and professional services on an SLA basis from the Cloud Provider, as described in the Pricing Schedule;

"**Secret Storage Service**" – a service that enables the Cloud Customer to store secrets, such as passwords or keys, to allow authenticated access to those secrets by their own systems or other services of Catalyst Cloud;

"**Usage Costs**" – a service which allows the Cloud Customer to explore the usage and cost of resources in real time and with history of usage over time;

"**VPN Service**" – a service that enables the Cloud Customer to provision Virtual Private Network connections between virtual routers and third parties using standards-based protocols.

4. General Terms and Conditions for all Cloud Services

4.1 The following terms of service apply to all offerings of **Cloud Services** in addition to any terms for the specific service defined in this agreement (including those defined in the appendices);

4.2 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;

4.3 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:

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

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

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

4.3.4 Implementation of any security policies, practices, or controls for any resources or configuration of their usage of the cloud, including but not limited to operating system configuration of servers they have access to, network filtering, and securing any keys or authentication credentials needed to access the platform or resources they have created within the

platform.

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

4.5 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;

4.6 The Cloud Provider reserves the right to perform emergency maintenance at any time to resolve any critical, necessary or significant matters such as fault, 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

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

4.8 Where there is no reference to an Agreed Service Level for a service, including when there are no service-specific terms for the service, the Cloud Customer accepts there is no Agreed Service Level for the service, and no Service Level Credits can be requested for that service.

4.9 Encryption performed by the Cloud Provider on Cloud Data and/or network traffic, either with keys managed by the Cloud Provider or keys provided by the Cloud Customer to the Cloud Provider, will not be provided to any third party, except as required under disclosure clauses in this agreement.

4.10 The Cloud Customer accepts and acknowledges that in relation to services designated as Beta:

4.10.1 The services are incomplete, undergoing testing or development, and are not recommended by the Cloud Provider for any workload;

4.10.2 That changes to the service do not require any notification to the Cloud Customer, regardless of the nature of the change;

4.10.3 That the service may contain known bugs and issues, and no Agreed Service Level applies, nor any right of credit for interruptions, loss, or incorrect behaviour of the service; and

4.10.4 The Cloud Provider has no obligation or agreed time frame for the service to be designated Generally Available.

4.11 The Cloud Customer accepts and acknowledges that in relation to services designated as Technical Preview:

4.11.1 The services are under a high rate of development and testing, and are not recommended by the Cloud Provider for any workload;

4.11.2 Subject to change or removal of any API or feature within an API, behaviour or capability without limitation and without notice of change to the Cloud Customer;

4.11.3 May be limited to approved Cloud Customers, entirely at the Cloud Provider's sole discretion, which may be revoked at any time and for any reason without notice or explanation to the Cloud Customer;

4.11.4 May be withdrawn at any time and for any reason, without notice, and with no obligation to provide any alternative service or method of a similar or related capability; and

4.11.5 There no obligation or agreed time frame for the service to be designated as Beta or Generally Available by the Cloud Provider.

5. Credit Request and Claim Procedure

5.1 Subject to clause 5.2, where the Cloud Provider has not met an Agreed Service Level

for a Cloud Service in a given month, the Cloud Customer shall be entitled to the Service Level Credits defined under the specific Cloud Service affected.

5.2 The Cloud Customer shall not be entitled to Service Level Credits if:

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

5.2.2 The Service failure was caused by a misuse of the Cloud Service by the Cloud Customer, whether the Cloud Customer authorised this use or otherwise;

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

5.2.4 The event occurred during Scheduled Maintenance;

5.2.5 The Cloud Customer fails to file a claim in time or provide sufficient information as described in clause 5.3; or

5.2.6 The Cloud Customer fails to provide in a timely manner other supporting information requested by the Cloud Provider on a reasonable basis to assist with identifying the cause of the breach.

5.3 To receive Service Level 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 Agreement item. The request must include:

5.3.1 The dates and times of each Unscheduled Outage;

5.3.2 The IDs of the affected Cloud Services; and

5.3.3 Any information or error logs that support the claim.

5.4 The Cloud Provider will credit Service Level Credits to the Cloud Customer's account upon confirming that the relevant Agreed Service Level item has not been met.

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

6. Violation of Service Terms

6.1 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.

7. Confidentiality

7.1 The Cloud Provider recognises that the Confidential Information is confidential, and agrees that:

7.1.1 The Cloud Data is designated as Confidential Information; and

7.1.2 The Cloud Data is the property of the Cloud Customer

7.2 Except to the extent permitted under these Services 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 use the Confidential Information solely for the purposes of the Cloud Agreement and not for any other purpose.

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

8. Data Collection

8.1 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.

8.2 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.

8.3 The Cloud Customer recognises that:

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

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

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

8.4 The Cloud Customer acknowledges and accepts that the Cloud Provider will store the Cloud Data in accordance with Clause 9.1, 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 in the same country as the Cloud Customer uploaded the data to, and the Cloud Customer agrees that the Cloud Provider is deemed to be the intended recipient of the Cloud Data.

9. Data Protection

9.1 The Cloud Customer acknowledges and accepts that:

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

9.1.2 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.

9.2 In accordance with Clause 9.1.1, 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.

9.3 In accordance with Clause 9.1.2, 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.

10. Use of Data

10.1 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.

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

10.3 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 2020.

10.4 The Cloud Provider will not access Cloud Data from outside New Zealand, unless written permission has been obtained beforehand.

10.5 The Cloud Provider will not transfer unencrypted Cloud Data outside New Zealand, unless written permission has been obtained beforehand.

11. Disclosure of Data

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

11.1.1 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;

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

11.1.3 That third party has signed a non-disclosure agreement or an agreement containing a non-disclosure provision.

11.2 With the exception of clause 11.1 and 11.3, the Cloud Provider shall not disclose Confidential Information to any other third party unless:

11.2.1 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;

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

11.2.3 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

11.2.4 For any other lawful purpose in accordance with the Privacy Act 2020.

11.3 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:

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

11.3.2 Attempt to refer the request for disclosure to the Cloud Customer; and

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

11.4 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:

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

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

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

11.5 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.

11.6 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 11.6 clause does not restrict the Cloud Provider.

12. Data Storage

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

12.2 The Cloud Provider agrees:

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

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

12.2.3 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

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

12.3 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.

12.4 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.

12.5 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.

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

13. Security Audits

13.1 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.

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

13.3 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.

14. Account Security

14.1 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.

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

14.3 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.

14.4 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.

15. Security – Breach Notification

15.1 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:

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

15.1.2 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;

15.1.3 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

15.1.4 The Cloud Provider will consider 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.

15.2 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.

Appendix A: Control Plane Specific Terms

A.1. The following terms of service in this section apply only to the **Control Plane**.

A.2. The Control Plane service is designated as Generally Available.

A.3. The Cloud Customer acknowledges that, in general, outages of the Control Plane do not affect the availability of other Cloud Services;

A.4. The Cloud Customer acknowledges that the Control Plane may not be available for use from time to time for reasons including but not limited to maintenance, upgrade, repair, fault, or failure; and

A.5. The Cloud Provider will take reasonable steps to minimise any disruptions or interruptions to the use of the Control Plane, noting there is no Agreed Service Level for this service.

Appendix B: Block Storage Service Specific Terms

B.1. The following terms of service in this section apply only to the **Block Storage Service**.

B.2. The Block Storage Service is designated as General Available.

B.3. Cloud Data stored in the Block Storage Service is encrypted at rest by the Cloud Provider, using keys that the Cloud Provider holds and manages, with the exception of Cloud Data stored in the Wellington region which is not encrypted at rest.

B.4. Cloud Data stored using the Block Storage Service employs techniques that reduce the possibility of loss of data due to a failure in the Cloud Provider's hardware or software. However, Cloud Data is stored at the Cloud Customer's risk, and the Cloud Customer is responsible for ensuring that sufficient backups are made of any Cloud Data, and that these backups are able to be used to restore any data lost.

B.5. The Cloud Provider shall undertake all reasonable efforts to meet the Agreed Service Level for the Block Storage Service, which excluding all Scheduled Outages is a Monthly Uptime Percentage of 99.95% for volume types with a replication factor of three (3). There is no SLA for volume types with a replication factor of two (2):

B.6. Where the Cloud Provider has failed to meet the Agreed Service Level for the Block Storage Service as defined in clause B.5, the Cloud Customer shall be entitled to Service Level Credits for the affected block storage volumes only, in accordance with the following table:

Monthly Uptime Percentage	**Service Level Credit**
Less than 99.95%, but greater or equal to 99.00%	20%
Less than 99.00%, but greater or equal to 95.00%	30%
Less than 95.00%	50%

Appendix C: Compute Service Specific Terms

C.1. The following terms of service in this section apply only to the **Compute Service**.

C.2. The Compute Service is designated as Generally Available, except for specific instance flavours which may be designated Beta or Technical Preview, as noted in sections C.6 and C.7 below.

C.3. The Cloud Customer is responsible for:

C.3.1. Ensuring that any operating system, operating system component, or software installed within the compute instance is compatible with or otherwise functional with the flavour of instance chosen by the customer including any virtualised, pass-through, or paravirtualised hardware components provided by the Compute Service.

C.3.2. The functional behaviour of any operating system, operating system component, or software installed in the compute instance where the Compute Service limits or reduces the execution time of the compute instance.

C.3.3. The configuration of the Cloud Customer's compute instances, including but not limited to any configuration, process, or monitoring that would enable it to start up automatically where there is a server failure irrespective of cause;

C.3.4. For managing the compute instance and any and all matters relating to the operating system and any other software within the compute instance, such as patching and maintaining security posture, regardless of who supplied that operating system or software; and

C.3.5. Ensuring that any operating system or software installed within the compute instance is licensed by the Cloud Customer, whether the cost of this license is included in charges by the Cloud Provider or otherwise.

C.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 from the configuration of a compute instance, any software running within the compute instances regardless of who provided that software, or from any server failure or from restarting compute instances;

C.5. The Cloud Provider will use reasonable efforts to meet the Agreed Service Level for the compute service, which excluding all Scheduled Outages is defined as a Monthly Uptime Percentage of 99.95%, as measured by the Cloud Provider's monitoring service at the hypervisor level, with the following exceptions:

C.5.1. The Cloud Customer accepts that the Cloud Provider has not breached the Agreed Service Level if the operating system or software within the compute instance is not functioning properly or is not configured in a manner which allows access, regardless of cause;

C.5.2. The Cloud Customer accepts that the Cloud Provider has not breached the Agreed Service Level if the execution time of the compute instance is less than one hundred percent (100%) or less than the specified maximum execution time for the compute instance flavour, which-ever is lower

C.6. The instance flavours in the list below are designated as Technical Preview, and consistent with clause 4.11 do not have an Agreed Service Level:

- c2-gpu (all sizes)

C.7. The instance flavours in the list below are designated as Beta, and consistent with clause 4.10 do not have an Agreed Service Level:

- c1.c32r256
- c1.c32r512
- c1.c64r256
- c1.c64r512
- c1.c64r768

- c1.c64r1024
- c1.c64r1280
- c2-burst (all sizes)

C.8. Where the Cloud Provider has failed to meet the Agreed Service Level for the Compute Service, the Cloud Customer will be entitled to Service Level Credits for the affected compute instances only, in accordance with the table below:

Monthly Uptime Percentage	**Service Level Credit**
Less than 99.95%, but greater or equal to 99.00%	20%
Less than 99.00%, but greater or equal to 95.00%	30%
Less than 95.00%	50%

Appendix D: Direct Connect Service Specific Terms

D.1. The following terms of service in this section apply only to the **Direct Connect Service**.

D.2. The Direct Connect Service is designated as Beta, and is subject to clause 4.10 and all sub-clauses within.

D.3. The Cloud Provider shall provide one or more network ports ("Direct Connect Port") at an agreed location for the Direct Connect Service. The network ports shall be the point of demarcation between the responsibility of the Cloud Provider and the Cloud Customer;

D.4. The Cloud Customer is responsible for all networking services and equipment that connects to the Direct Connect Port, including but not limited to optics, cables, routers, and access equipment to the facility;

D.5. The Cloud Customer must meet all technical requirements of the Direct Connect service, including specifications on networking protocols and standards required to connect to the Direct Connect Port;

D.6. The Cloud Customer is responsible for all fees and charges relating to their connection to the Direct Connect Port;

D.7. The Cloud Provider may, at its sole discretion, shut down the Direct Connect Port in an emergency if it deems that the activity or usage of this port is the cause of any service outage, impacts, or reduction in capacity beyond reasonable levels. The Cloud Provider shall use reasonable commercial means to inform the Cloud Customer this has taken place, and shall work with the Cloud Customer to restore the connection as soon as practical.

Appendix E: Identity and Access Management Service Specific Terms

E.1. The following terms of service in this section apply only to the **Identity and Access Management Service**.

E.2. The Identity and Access Management Service is designated as Generally Available.

E.3. The identity and Access Management Service allow the Cloud Customer to control and delegate access to it account(s) to any person, third parties, services, and machines;

E.4. 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; and

E.5. For avoidance of doubt, the Cloud Customer shall also comply with the provisions outlined in clause 14 (“Account Security”).

Appendix F: Image Service Specific Terms

F.1. The following terms of service in this section apply only to the **Image Service**.

F.2. The Image Service is designated as Generally Available.

F.3. The Cloud Customer is solely responsible for:

F.3.1. Uploading media or machine images to the Image Service (with the exception of media or machine images provided by the Cloud Provider or its duly authorised agent);

F.3.2. Maintaining the security and protection of the images and controlling access to the images;

F.3.3. Determining whether an image is fit for purpose and suitable for the Cloud Customer's use; and

F.3.4. Ensuring any usage or access to the image is consistent with any license attached to the content of the image, including entering into license agreements for any distribution or usage.

F.4. Images uploaded or created in the Image Service are private to the Customer by default. However, the Cloud Customer acknowledges that should they enable sharing for an image, the data contained within that image will be available to view, use, download, and otherwise by other Cloud Customers indefinitely and without the ability to remove or restrict any copies or use made of that image, and that the Cloud Provider has no responsibility for any loss of privacy, intellectual property breach, or breach of confidentiality as a direct or indirect result of the sharing of an image.

F.5. Where the Cloud Customer has uploaded or created an image to be stored by the Image Service, the Cloud Customer accepts that the content of images is stored at the Cloud Customer's risk, and that the Cloud Customer is solely responsible for ensuring that appropriate backups are made of the content such an image.

Appendix G: Kubernetes Service Specific Terms

G.1. The following terms of service in this section apply only to the **Kubernetes Service**.

G.2. The Kubernetes Service is designated as Generally Available.

G.3. 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:

G.3.1. Providing support for at least three minor versions of Kubernetes, allowing customers at least six months time to plan and perform upgrades;

G.3.2. Providing security updates for the base operating system, the Docker Engine and/or Kubernetes, in the form of new template versions;

G.3.3. 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);

G.3.4. Notifying customers about known critical security vulnerabilities and updates, by reasonable commercial means; and

G.3.5. Monitoring the availability of the Kubernetes clusters and resolving incidents impacting the control plane, master or worker nodes.

G.4. Cloud Customers are responsible for:

G.4.1. The software, configuration and Cloud Data in containers deployed to Kubernetes, including security updates and upgrades of these applications;

G.4.2. Any configuration, metadata or secrets stored in Kubernetes;

G.4.3. Performing major or minor upgrades, at a time appropriate for its business, using the provided upgrade API; and

G.4.4. Any intellectual property license required by the content of any container deployed to a cluster, except software pre-configured by the Cloud Provider as part of the provisioning or maintenance of the cluster.

G.5. Cloud Customers are recommended to:

G.5.1. Use highly available clusters (using a "production" cluster template provided by the Cloud Provider with at least three master nodes) for production workloads;

G.5.2. 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;

G.5.3. 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 a database;

G.5.4. 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; and

G.5.5. 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 exempts the Cloud Provider from incidents caused by them.

G.6. 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).

G.7. The Cloud Provider will use reasonable efforts to allow customers to upgrade from a Cloud Provider supported version of Kubernetes to another Cloud Provider supported version, but does not warrant that such upgrades can be performed without modification to the configuration of the cluster, any workload or workload definitions, nor without any interruption of service, nor with any assurance that upgrade will be successful under any and all circumstances, and that such upgrades are performed entirely the Cloud Customer's risk.

G.8. The Cloud Customer acknowledges that when upgrading between minor or major versions of Kubernetes, they may be required to upgrade to the immediate next version, and may not be able to skip minor or major versions in an upgrade process.

G.9. The Cloud Customer acknowledges and accepts that where the Cloud Customer is not running a Cloud Provider supported version of Kubernetes, there is no obligation on the Cloud Provider to support any version upgrade of Kubernetes, including but not limited to minor and major versions of Kubernetes whether the target version is supported by the Cloud Provider or not.

G.10. The Cloud Provider will use reasonable efforts to meet the Agreed Service Level for the Kubernetes Service, which excluding all Scheduled Outages is defined as a Monthly Uptime Percentage of 99.95% for the Kubernetes APIs (control plane) when deployments have been configured as highly available with three or more master nodes. For deployments not configured as highly available there is no Agreed Service Level. The Agreed Service Level for individual worker nodes is covered by the Compute Service Agreed Service Levels.

G.11. Where the Cloud Provider has failed to meet the Agreed Service Level for the Kubernetes Service, the Cloud Customer will be entitled to Service Level Credits for the affected cluster only, in accordance with the table below:

Monthly Uptime Percentage	Service Level Credit
Less than 99.95%, but greater or equal to 99.00%	20%
Less than 99.00%, but greater or equal to 95.00%	30%
Less than 95.00%	50%

Appendix H: Load Balancer Service Specific Terms

H.1. The following terms of service in this section apply only to the **Load Balancer Service**.

H.2. The Load Balancer Service is designated as Generally Available.

H.3. The Cloud Provider is responsible for:

H.3.1. Applying security updates to the base operating system and/or software that provides the load balancing service;

H.3.2. Notifying customers of any known critical security vulnerabilities that would fail to enforce any configuration that the customer has specified, by reasonable commercial means;

H.3.3. 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;

H.3.4. Ensuring that traffic that traverses the load balancer is not modified unless the Cloud Customer has explicitly configured the load balancer to do so; and

H.3.5. Protecting the load balancer operating system from unauthorised access.

H.3.6. Where the Cloud Customer has configured the use of TLS termination, that the keys used to provide the TLS termination are protected from unauthorised access by third parties.

H.4. The Cloud Customer is responsible for:

H.4.1. 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;

H.4.2. Configuration of health checks in the load balancer to inform the load balancer of what targets are able to be used;

H.4.3. 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;

H.4.4. Defining any restrictions on address ranges which may direct traffic towards the load balancer;

H.4.5. 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;

H.4.6. Ensuring the security of any system that is a target of the load balancer;

H.4.7. Determining if the load balancer shall have a public IP address associated with it, for reception of traffic from the public Internet;

H.4.8. 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;

H.4.9. Where the Cloud Customer has configured TLS termination, definition of TLS versions to accept, algorithms, and any other security controls TLS termination may provide; and

H.4.10. Where the Cloud Customer has configured TLS termination, the validity or recognition of TLS certificates.

H.5. Cloud Customers are recommended to:

H.5.1. Maintain suitable logs of access to targets, where possible using additional information inserted by the load balancer on the original origin of the traffic;

H.5.2. Avoid attaching public IP addresses to load balancers that are intended to be private;

H.5.3. Limit the ports that a load balancer is configured to accept traffic on to only those required by their application(s);

H.5.4. Configure the load balancer to reject connections from IP addresses outside specific address ranges; and

H.5.5. 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.

H.5.6. Where TLS termination is configured, ensure that the certificates used are compliant with best practices for algorithms, lengths, and rotated on a regular basis.

H.6. Where TLS termination is configured, the Cloud Customer acknowledges that this service will access secrets or key material stored by the customer in the Secret Storage Service on the customer's behalf, and the Cloud Customer is responsible for the configuration of any access controls to the Secret Storage Service to enable the Load Balancer Service to access secrets configured for TLS termination.

H.7. 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 configuration of the load balancer as specified by the customer.

H.8. The Cloud Provider will use reasonable efforts to meet the Agreed Service Level for the Load Balancing Service, which excluding all Scheduled Outages is defined as a Monthly Uptime Percentage of 99.95% as measured by monitoring from the control plane of the service, and subject to clause H.9 below.

H.9. 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.

H.10. Where the Cloud Provider has failed to meet the Agreed Service Level for the Load Balancer Service, excluding Scheduled Outages, the Cloud Customer will be entitled to Service Level Credits for the affected load balancer instances only, in accordance with the following rules:

Monthly Uptime Percentage	**Service Level Credit**
Less than 99.95%, but greater or equal to 99.00%	20%
Less than 99.00%, but greater or equal to 95.00%	30%
Less than 95.00%	50%

Appendix I: Object Storage Service Specific Terms

I.1. The following terms of service in this section apply only to the **Object Storage Service**.

I.2. The Object Storage Service is designated as Generally Available.

I.3. Cloud Data stored in the Object Storage Service is encrypted at rest and the Cloud Provider holds and manages the encryption keys;

I.4. The Cloud Customer may choose whether to distribute data uploaded to a specific object container across three regions, or contained within a single region, noting that:

I.4.1. The Cloud Customer takes responsibility for the choice of whether to distribute object data across multiple regions; and

I.4.2. Distribution of data to different regions is performed asynchronously, and there is a delay between when the data upload was completed and when the data will be distributed to other regions;

I.5. The Cloud Customer accepts that Cloud Data stored in the Object Storage Service is at the Cloud Customer's risk, and that they are solely responsible for ensuring appropriate backups are made of any Cloud Data stored in the Object Storage Service.

I.6. The Cloud Provider will use reasonable efforts to meet the Agreed Service Level, defined as a Monthly Uptime Percentage of 99.9% for the Object Storage Service, excluding Scheduled Outages.

I.7. Where the Cloud Provider has failed to meet the Agreed Service Level for the Object Storage Service, the Cloud Customer will be entitled to Service Level Credits for the affected object storage containers only, in accordance with the following table below:

Monthly Uptime Percentage	Service Level Credit
Less than 99.95%, but greater or equal to 99.00%	20%
Less than 99.00%, but greater or equal to 95.00%	30%
Less than 95.00%	50%

Appendix J: VPN Service Specific Terms

J.1. The following terms of service in this section apply only to the **VPN Service**.

J.2. The VPN Service is designated as Beta, and subject to the conditions of clause 4.10 and all sub-clauses of that clause.

J.3. The Cloud Customer is responsible for:

J.3.1. Monitoring the state of the VPN connection, where necessary from both ends of the connection;

J.3.2. Ensuring the configuration of the VPN is correct for both ends;

J.3.3. Any interoperability issues between the VPN Service and a third party VPN endpoint;

J.3.4. Defining the security requirements of the connection are met by the VPN Service;

J.3.5. Management of any keys or secrets associated with the VPN Service;

J.3.6. Ensuring that any keys or secrets are not disclosed to any other party except as is required to establish the VPN connection; and

J.3.7. Any network changes required on either side of the connection which enable the connection to be used appropriately.

Appendix K: Managed Database Service Specific Terms

K.1. The following terms of service in this section apply only to the **Managed Database Service**.

K.2. The Managed Database Service is designated Generally Available.

K.3. The Cloud Customer is responsible for:

K.3.1. Selecting the database engine that is appropriate to their desired use;

K.3.2. Ensuring the size of the instance(s) is suitable for the workload being placed on the database;

K.3.3. The schema, content, and data of any database within a database instance;

K.3.4. User management, access controls, credentials, and permissions within the database instance, even when these can be driven by the Managed Database Service;

K.3.5. Ensuring data is protected appropriately while at rest in the database instance;

K.3.6. The configuration and execution of any data backup and restoration processes even when some aspect of these services is provided by the Managed Database Service;

K.3.7. Validation of any backed up data and usability for restoration of any services according to the Cloud Customer's needs;

K.3.8. Configuration of any replication requirements for the Cloud Customer's needs, whether provided by the Managed Database Service or otherwise;

K.3.9. Sizing of the data storage volumes to ensure that sufficient space is available for the Cloud Customer's workloads and usage of the database engine;

K.3.10. The selection of a data storage volume type that ensures sufficient performance for the Cloud Customer's needs;

K.3.11. Monitoring of the database instance(s) to ensure they are available, including automatically starting or stopping instance(s) as required for any reason;

K.3.12. Configuration of any application to establish a connection to a database instance, including where this configuration must reflect different instances in a replication arrangement;

K.3.13. The provision and operation of any management tools required to effectively manage the database engine, such as maintenance of schema;

K.3.14. The definition of any configuration items that the Managed Database Service can inject into the database instance, with the exception of parameters that are automatically generated by the Database service as noted in the Technical Documentation;

K.3.15. Archival practices for data to ensure performance;

K.3.16. Query design and implementation from applications or other software for performance and correctness;

K.3.17. Upgrading the database engine using the API provided for minor upgrades on a schedule of the Cloud Customer's own determination;

K.3.18. Migration of database to a new major version, including any provisioning of new instance(s) and data copying or transformation required to use the new major version;

K.3.19. Ensuring that the database engine is updated or protected from unauthorised access to address any security issues, whether a minor upgrade

is available or otherwise;

K.3.20. The configuration of any network access controls to limit access to the database instance; and

K.3.21. Monitoring of the replication state and delay in any configuration of replication of database content or schema.

K.4. The Cloud Provider is responsible for:

K.4.1. The security and configuration of the underlying operating system supporting the database engine;

K.4.2. Building and providing images suitable to launch a supported database engine;

K.4.3. Ensuring that instances are isolated from other Cloud Customers;

K.4.4. Ensuring automatically generated configuration items are correctly generated when inputs change (e.g., sizing of instances by the Cloud Customer); and

K.4.5. Notifying customers of the end support by the Cloud Provider for a major version of a database engine at least six (6) months before the end of support.

K.5. The Cloud Customer accepts that Cloud Data stored in the Managed Database Service is at the Cloud Customer's risk. The Cloud Customer acknowledges that while the service provides an automatic backup system, these backups are also stored at the Cloud Customer's risk, and they are solely responsible for ensuring backups outside the service are created as required.

K.6. The Cloud Provider will use reasonable efforts to meet the Agreed Service Level, defined as a Monthly Uptime Percentage of 99.95% for the Managed Database Service, excluding Scheduled Outages, as measured by the control plane reporting a healthy state of a database instance, treating each replica (if configured) as a

separate instance, subject to clause K.7.

K.7. The database instance is deemed to be available regardless of replication state, consistent with K.3.21.

K.8. Where the Cloud Provider has failed to meet the Agreed Service Level for the Managed Database Service, the Cloud Customer will be entitled to Service Level Credits for the affected cluster only, in accordance with the table below:

Monthly Uptime Percentage	**Service Level Credit**
Less than 99.95%, but greater or equal to 99.00%	20%
Less than 99.00%, but greater or equal to 95.00%	30%
Less than 95.00%	50%

Appendix L: Ingress Protection Service Specific Terms

L.1. The following terms of service in this section apply only to the **Ingress Protection Service**.

L.2. The Ingress Protection Service is designated as Generally Available.

L.3. The Cloud Customer accepts that:

L.3.1. All incoming traffic from the Internet will be subject to the Ingress Protection Service, and that this cannot be disabled;

L.3.2. Traffic within the Cloud Provider's network, including networks created by the Cloud Customer, are not subject to the Ingress Protection Service;

L.3.3. Traffic that arrives at the Cloud Provider's network from a Direct Connect service connection are not subject to the Ingress Protection Service;

L.3.4. The Ingress Protection Service may prevent traffic from passing into the Cloud Customer's resources or the Cloud Provider's services from time to time, including situations where it is not the Cloud Customer that is being attacked;

L.3.5. The Ingress Protection Service may not prevent an attack from affecting the Cloud Customer or the Cloud Provider;

L.3.6. Incoming traffic from the Internet may not take the most direct path to the Cloud Provider in order to traverse the Ingress Protection Service;

L.3.7. Incoming traffic may not traverse the Ingress Protection Service from time to time, as required by maintenance, emergency procedures, or as a consequence of Internet routing protocols;

L.3.8. Incoming traffic from the Internet has no guarantee of remaining within New

Zealand, and may be inspected at a location outside New Zealand; and

L.3.9. The service, and consequently public Internet access, has no Agreed Service Level.

L.4. The Cloud Provider is responsible for:

L.4.1. Ensuring that appropriate monitoring takes place to ascertain the status and health of the Ingress Protection Service;

L.4.2. Specifying clearly the degree of inspection into traffic that any aspect of the Ingress Protection Service may apply in making decisions on whether to allow or deny traffic to reach the Cloud Customer or the Cloud Provider's network, while maintaining the Cloud Provider's obligations for encryption keys under clause 4.9;

L.4.3. Defining the policies and configuration of the Ingress Protection Service to mitigate attacks on the Cloud Customer and/or Cloud Platform, without any assurance that all attacks can be successfully mitigated or have no affect on the Cloud Customer and/or Cloud Platform; and

L.4.4. Where the Cloud Customer has a support agreement that includes notification of attacks mitigated or in progress, notifying the Cloud Customer of these occurrences.

L.5. The Cloud Customer is recommended to:

L.5.1. Design and deploy additional methods of mitigating attacks from the Internet to their resources and systems on the Cloud Provider's platform, such as a Web Application Firewall; and

L.5.2. Deploying encryption on services exposed to the Internet where it is appropriate to do so, to ensure that the Ingress Protection Service does not have visibility of data in transit that the Cloud Customer has an obligation to protect.

Appendix M: Secret Storage Service Specific Terms

M.1. The following terms of service in this section apply only to the **Secret Storage Service**.

M.2. The Secret Storage Service is designated Technical Preview, and subject to clause 4.11 and all sub-clauses within..

M.3. The Secret Storage Service allows a the Cloud Customer to store secrets (such as passwords or encryption keys) to be accessed by software running in their account or by other services operated by the Cloud Provider.

M.4. The Customer acknowledges that the following services from the Cloud Provider may interact with the Secret Storage Service on the customer's behalf:

M.4.1. Load Balancing Service (for the purpose of TLS termination using public and private keys provided by the Customer)

M.5. The Customer is responsible for:

M.5.1. Generating any secrets or key material, including the selection of length, strength, algorithms, randomness, source of entropy, or numerical constants used during generation;

M.5.2. Ensuring that the parameters used to generate secrets or key material is compatible with any software (including services provided by the Cloud Provider) that is expected to utilise the secret or key;

M.5.3. Arranging for any validation, signing, or verification of a secret or key by a third party if required for a specific use, for example TLS certificate signing;

M.5.4. Replacement of the secret or key material, or any associated validation of the secret or key material in a timely manner consistent with the Customer's own

policies on such replacement or the technical requirements of any validation, verification, or signing of the secret or key;

M.5.5. The definition of any attributes associated with the secret or key material, such as subject names or purposes encoded into the secret or key material;

M.6. The Cloud Provider is responsible for:

M.6.1. Ensuring that any secret or key material uploaded into the service is stored securely at rest;

M.6.2. Enforcing access control to the secret or key material;

M.6.3. Ensuring that any Cloud Provider service named in section M.4 above which accesses the secret or key material will not disclose the secret or key material to any third party, and utilises the secret or key material only for the purpose for which it was provided;

M.7. The Cloud Customer accepts that secrets or keys stored in the Secret Storage Service are at the Cloud Customer's risk, and they are solely responsible for ensuring that backups exist of any secrets or keys stored in the Secret Storage Service.

M.8. As the Secret Storage Service is provided on a Technical Preview basis there is no Agreed Service Level provided for the service.

Appendix N: Audit Log Service Specific Terms

N.1. The following terms of service in this section apply only to the **Audit Log Service**.

N.2. The Audit Log Service is designated Technical Preview, and subject to clause 4.11 and all sub-clauses within.

N.3. The Audit Log Service delivers to the Cloud Customer a record of actions or events relating to one or more of their accounts with the Cloud Provider.

N.4. The format, meaning, or presence of these log entries may change at any time, without any requirement for the Cloud Provider to notify of such changes. The Cloud Customer may require additional information to interpret or derive meaning from the log entries.

N.5. Log entries are not provided in "real-time", and the Cloud Customer accepts and acknowledges that there is a unspecified and unknown delay between the event or action occurring and a log entry being made available to the Cloud Customer.

N.6. Log entries are not guaranteed to be in sequential order, or that a given log segment is all actions or events for a specific period.

N.7. When enabled at the Cloud Customer's request, log entries will be delivered to an Object Storage container that the Cloud Customer names. The Audit Log Service will then create directories or files in this Object Storage container, until the Cloud Customer requests the service be disabled.

N.8. Log entries delivered shall commence from the point the service is enabled until the point in time the service is disabled. The Cloud Provider will not provide log entries before the point in time the service was enabled, regardless of whether such log entries exist in any system or store.

N.9. Not every service, nor every action or event within that service, may result in a log entry. While the Cloud Provider will endeavour to capture every action or event, this

is not guaranteed and some may not be provided to the Cloud Customer. A list of supported services and scope is provided on the Cloud Providers website.

N.10. The Cloud Customer is responsible for:

N.10.1. Ensuring the security and access controls of the Object Storage container which the Audit Log Service will place logs into;

N.10.2. Configuring any access controls on the Object Storage container to allow the Audit Log Service to deposit logs;

N.10.3. Any integration with any software or process to interpret, aggregate, or otherwise process the logs.

N.10.4. Removing from the Object Storage container any logs which are not longer required to be retained.

N.11. The Cloud Provider is responsible for:

N.11.1. When the Cloud Customer has requested logs be generated, those logs are generated and stored in the specified Object Storage container in a reasonable amount of time.

Appendix O: DNS Hosting Service

O.1. The following terms of service in this section apply only to the **DNS Hosting Service**.

O.2. The DNS Hosting Service is designated Technical Preview, and is subject to clause 4.11 and all sub-clauses within.

O.3. The DNS Hosting Services enables a Cloud Customer to manage DNS Zones and Record Sets using API calls or interaction with the Dashboard. The Zones and Record Sets will be served by Authoritative Nameservers provided by the Cloud Provider, except as noted below.

O.4. This section does not apply to any other DNS services, including but not limited to nameservers provided to Customers by the Cloud Provider for resolving DNS names (so called "recursive nameservers").

O.5. In this section and only this section, unless the context requires otherwise:

"**Authoritative Nameserver"** means a nameserver that will respond only to queries for zones it has been configured to answer, and will not proxy, relay, or recursively resolve queries to any other nameservers on the Internet.

"**Cache time**" means either the Time To Live of a Record Set, or any of the caching elements of the "SOA" record type.

"**Delegation**" means the the technical configuration of a zone to partition a sub-domain of that zone to another set of nameservers.

"**DNS**" means the Domain Name System, as defined by the DNS Standard.

"**DNS Standard**" means the collection of IETF RFCs and Best Practices that collectively define the "Domain Name System" and related subject areas, including but not limited to RFC 1034 and RFC 1035.

"**Nameserver**" means the technical function to respond to queries using DNS protocols, either on a recursive or authoritative basis..

"**Record Set**" means one or more answers for a specific DNS query.

"**Record Type**" means a type of DNS query and record set as defined by DNS Standards

"**Recursive Nameserver**" means a nameserver that given a query will consult its own cache of queries and answers, before querying the global Root and follow all delegations found to attempt to answer a query..

"**Root**" means the set of DNS Nameservers operated by the Internet Corporation for Assigned Names and Numbers (ICANN), that forms the top of the DNS tree.

"**Serial Number**" means the "Serial" element of the SOA Record Set type on the Zone Apex.

"**TLD Registry**" means an organisation that has been delegated authority to operate a "top-level domain" as defined and nominated by the Internet Corporation for Assigned Names and Numbers (ICANN).

"**Zone**" means a portion of the DNS namespace that is managed by a specific person or organisation, and contains Record Sets.

"**Zone Apex**" means the Record Sets that are defined for the zone name itself.

O.6. The Cloud Customer acknowledges that:

O.6.1. The Cloud Customer may need to understand the function, protocols, and implementation of the Domain Name System in order to utilise the DNS Hosting Service provided by the Cloud Provider.

O.6.2. Not all Record Types or behaviours defined in the DNS Standards may be supported by the DNS Hosting Service.

O.6.3. The DNS Service may allow Record Sets which are not compliant with the DNS Standard, and consequently may not able to be correctly utilised by any other DNS implementation

O.6.4. The DNS Service does not ensure that any other system connected to the

Internet can usefully or correctly interpret the answer given to a DNS query.

O.6.5. Cache times set by the Customer on any Record Set or the SOA Record Set on the Zone Apex may or may not be honoured by any other DNS implementation (including any Recursive Nameserver provided by the Cloud Platform), and a Record Set or Zone may be cached for an undefined period of time (including not cached at all).

O.6.6. The Cloud Provider has no means, ability, or willingness to force any other DNS implementation (including the Cloud Provider's Recursive Nameservers) to clear caches or otherwise refresh updated records.

O.6.7. Changes to Record Sets made by the Customer may not be immediately reflected in queries sent to the Cloud Provider's DNS Hosting Nameservers.

O.6.8. The Cloud Provider may, from time to time, change the names or IP addresses of the Authoritative Nameservers that queries should be pointed towards. As the DNS Service is classed as Technical Preview, Customers may not be given any advance notice of these changes.

O.6.9. The Cloud Provider has no responsibility for the operation or correct behaviour of the Root or any nameservers in the delegation path (including TLD Registry nameservers), or those of any provider of services involving the Internet behaviour with regards to the resolution of a DNS query.

O.6.10. The Cloud Provider has no responsibility to validate, obtain proof, or otherwise ensure that a Cloud Customer has authority to control the Zone or any content of the Zone.

O.7. The Cloud Customer is responsible for:

O.7.1. Any and all technical requirements, fees, contracts, agreements, or other matters that a either a TLD Registry or any other nameserver in the delegation path requires of the Cloud Customer to retain control over any Zone.

O.7.2. Ensuring that the correct DNS names and IP addresses are used at all times for delegation records in a TLD Registry's nameservers or that of any nameserver in the delegation path, to effect pointing DNS queries to the Cloud Provider's Authoritative Nameservers.

O.7.3. The choice of domain name for a Zone, and the content and correctness of any Record Sets within a Zone that is created and managed in the DNS Hosting Service.

O.7.4. Specifying the Zone's SOA record content, except for the Serial Number, which will be generated by the Service as noted in section O.8.7.

O.8. The Cloud Provider is responsible for:

O.8.1. Operating the Authoratitive Nameservers that a Cloud Customer's Zone and Record Sets are hosted by, including but not limited to any operating system, software, or configuration required to implement the service.

O.8.2. Publishing current information on the DNS names and IP addresses of the Authoritative Nameservers used to host the Cloud Customer's Zone and Record Sets.

O.8.3. Ensuring that at least one (1) Authortaitive Nameserver is available and responding to DNS queries at all times.

O.8.4. Reflecting changes made to Record Sets in a Cloud Customer's Zone are served from all Authoritative Nameservers within a reasonable amount of time, without assurance that the change will be effected on all Authoritative Nameservers at the same moment.

O.8.5. Answering DNS queries that reach the Authoritative Nameservers with the content of the Cloud Customer's Zone and Record Sets, or with a negative response when the query cannot be satisfied by the content provided.

O.8.6. Ensuring that the Authoritative Nameserver does not modify, alter, or enrich

the response to a query to be different from the Record Set that the Cloud Customer has provided for that name, except where such modification is required, recommended, or acceptable within the DNS Standard.

O.8.7. Generating a Serial Number in the SOA record for a Zone, that is incremented on each change in Record Sets for a Cloud Customer's Zone.

O.9. The Cloud Provider may, at its sole discretion and at any time, refuse or remove a Zone that it deems a breach of the Acceptable Use Policy of the Cloud Provider, in accordance with the breach process of the Acceptable Use Policy.

O.10. The Cloud Customer warrants that by creating a Zone in the DNS Hosting Service it has the legal authority to control the content of that Zone.

O.11. The Cloud Customer will indemnify the Cloud Provider on demand against any losses suffered or incurred by the Cloud Provider arising out of or in connection with claim, dispute process, or court process made by another person or organisation relating to the control of that Zone.

O.12. If the Cloud Provider receives notice of a claim relating to the Cloud Customer's authority to control the Zone or the contents of the Zone, the Cloud Provider may at its absolute discretion suspend or remove the Zone from the DNS Hosting Service .

O.13. In the case of a dispute between the Cloud Customer and any other party relating to a Zone hosted by the DNS Hosting Service, the Cloud Provider will have no responsibility of any kind to the Cloud Customer in relation to such dispute.

END OF DOCUMENT