CloudCode of Practice Disclosure Statement

Catalyst Cloud Limited

Table of contents

Document control

Owner	Andrew Ruthven
Classification	Public
Reviewed By	David Zanetti
Approved By	Paul Seiler
Status	Published
Last Review	2022-11-30
Next Review	2023-11-29
Review Period	Annual
Source	Alfresco - Catalyst Cloud / CloudCode / Catalyst Cloud - CloudCode Disclosure Statement.odt
Published	https://catalystcloud.nz/about/privacy-and-compliance/

Revision history

Version	Date	Description/notes	Author(s)
1.0	2015-02-02	Published	Bruno Lago
1.1	2021-09-07	Updated to reflect separation of Catalyst Cloud into Catalyst Cloud Limited. Add PCI DSS, Hamilton region, reduce CSA STAR, add ISO 27001 work, update services.	Andrew Ruthven
1.2	2021-09-15	Add ISO 27001 and 27017 certification	Andrew Ruthven
1.3	2022-11-30	Extend backup period, add Audit Log and Load Balancer Reviewed by David Zanetti, no changes.	Andrew Ruthven

1 Disclosure

For an organisation to be a CloudCode Signatory they must wholly disclose the following information to all clients, both prospective and current, before, during and after the sales process. They must update their Disclosure Document and inform the Register of CloudCode Signatories of these changed disclosures as soon as possible and not later than 28 days after the change is made. Where the change has a material effect on the Cloud product or service being provided, they must notify all clients of these changes.

The CloudCode website provides more information of what constitutes a material change. The standard areas of disclosure required by the CloudCode are:

2 Corporate Identity

Knowing who you are doing business with and how to contact them is an important part of building trust.

Company name:	Catalyst Cloud Limited
Company Registration Number:	6276828
Trading name:	Catalyst Cloud
Physical address:	Level 6, Catalyst House, 150 Willis St, Wellington 6011
Postal address:	PO Box 11053, Manners St, Wellington 6142, New Zealand
Company website:	www.catalystcloud.nz
Contact phone number:	+64 (0) 800 2282 5683
Contact email address:	enquiries@catalystcloud.nz

Complaints about our service can be made in the first instance to: sales@catalystcloud.nz

Contact person responsible for these disclosure statements can be contacted via the following email address: security@catalystcloud.nz (Andrew Ruthven).

The disclosures herein apply to the following products or services supplied by us:

- **Compute Service** as described at **https://catalystcloud.nz/services/iaas/compute/**
- **Image Service** as described at **https://catalystcloud.nz/services/iaas/image/**
- **Block Storage** as described at **https://catalystcloud.nz/services/iaas/block-storage/**
- **Object Storage** as described at **https://catalystcloud.nz/services/iaas/object-storage/**

- **Network** as described at **https://catalystcloud.nz/services/iaas/network/**
- **Load Balancer** as described at **https://catalystcloud.nz/services/iaas/load-balancer/**
- **VPN-as-a-Service** as described at **https://catalystcloud.nz/services/iaas/vpn/**
- **Direct Connection** as described at **https://catalystcloud.nz/services/iaas/direct-connection/**
- **Alarm** as described at **https://catalystcloud.nz/services/paas/alarm/**
- **Cloud Orchestration** as described at **https://catalystcloud.nz/services/paas/cloud-orchestration/**
- **Kubernetes** as described at **https://catalystcloud.nz/services/paas/kubernetes/**
- **Managed Database** as described at **https://catalystcloud.nz/services/paas/managed-database/**
- **Ingress Protection (Distributed Denial-of-Service)** as described at **https://catalystcloud.nz/services/paas/ingress-protection/**
- **Identity & Access Management (IAM)** as described at **https://catalystcloud.nz/services/management/iam/**
- **Usage Costs** as described at **https://catalystcloud.nz/services/management/usage-costs/**
- **Audit Log** as described at **https://catalystcloud.nz/services/management/audit-log/**

For the purpose of Legal Jurisdiction, the contracted supplier who provides the service to you is a **Cloud Service Provider** registered in **New Zealand**.

The governing law of our contract with you is **New Zealand**.

The disclosure statements that follow have been **Self Assessed**.

3 Ownership of Information

The ownership of data and information supplied by the client to the service provider needs to be clearly disclosed, to ensure the rights to use the information are clearly understood. This section helps identify who owns client data, and data generated by the service provision.

- We **do not** claim ownership of any data or information uploaded to our service.
- We **do not** claim ownership of any data generated by the client (stored on compute instances, block storage or object storage) during or as a result of the use of our service.
- Your data and information may traverse or be stored on our upstream provider's networks or systems. In these instances those provider considers the data and information that you use or transmit via our service as owned by the **client**.
- Metadata and other statistical information, such as anonymised data generated as a result of the use of our service, is owned by the **service provider** and **may be** used for the purposes of **usage statistics, traffic modelling, performance analysis, providing the cloud services, and**

improving our services.

4 Security

Ensuring that a cloud service provider has a good set of standards and practice surrounding security is important. Although optional to become a Signatory, we recommend that Cloud Service Providers list on the CSA STAR Registry (see Appendix A).

As at the current date:

- We are **not** listed on the CSA STAR Registry.
- We are formally meet the following information security standards: **ISO 27001:2013** and **ISO 27017:2015** which have been externally assessed and audited by **BSI**. The certificates are available from: https://catalystcloud.nz/about/privacy-and-compliance/.
- We formally meet the following security related standard: **PCI DSS 3.2.1** (physical security for our Porirua and Wellington data centres) which have been externally assessed or audited by **Confide**. The certificate is available from: **https://catalystcloud.nz/about/privacy-and-compliance/**
- We formally meet the following security related standard: **PCI DSS 3.2.1** (physical security for our Hamilton data centre in a co-location facility) which have been externally assessed or audited by **Confide** for **our co-location provider**. The certificate is available upon request.
- We formally meet the following security related standard: **ISO 27001:2013** (physical security for our Hamilton data centre in a co-location facility) which have been externally assessed or audited by **SAI Global Assurance** for **our co-location provider**. The certificate is available upon request.

5 Data Location

Cloud Service Providers may host data on a number of servers, located locally or offshore. Knowing where hosted data is located can help customers assess any risks or benefits for their business. Please note that any legal jurisdictions over data and information may change depending on the location.

- Our primary systems that host your data are located in **New Zealand**.
- Our Backup/Disaster Recovery systems that hold your data are located in **New Zealand**.

Additional disclosures about data locations:

- Customers can choose any Catalyst Cloud region (Hamilton, Porirua or Wellington) as their primary location.

6 Data Access and Use

Knowing how customer data can be accessed both during and after a service has been provided is an important step to ensuring that, when a service has been ceased, the right provisions are made.

Data access by you:

- Your data may be accessed during the contract period as described in our contract with you.
- Your data can be downloaded from our service during the service provision period using the mechanisms specified in section 12 Data Formats.
- At the cessation of our service to you, your data **will not** be available to access.
    - Customers can download all their data before they request the service to be terminated.
    - Where we initiate termination of the service, for example due to a breach of the Terms and Conditions, we will have already taken reasonable steps to notify the customer and to negotiate a resolution to the termination trigger. We **may** choose to maintain data after termination where we consider agreement on a new service with the customer is likely.

Data access by us:

- Deletion of all customer data at the cessation of our service to you takes place **immediately, except where data must be retained for legal purposes**.
- We **do not** access customer data for any business purpose.
- We **do not** use customer data in order to generate revenue other than through provision of the service.

Data access by others:

- If we are approached by law enforcement agencies it is our policy to **comply with lawful requests that conform to legal obligations as determined by New Zealand law.**
- We **do not** provide access to customer data to third parties other than law enforcement agencies as set out above.

7 Backup and Maintenance

Understanding the backup procedures of your service provider and their maintenance policies allows the customer to make decisions on what further steps they may need to ensure their data is backed up sufficiently.

Backup of customer data stored in the Computer Service, Image Service, Block Storage or Object Storages services is available as an additional managed service via third parties available here: https://catalystcloud.nz/solutions/#backup-and-disaster-recovery. The standard cloud services do not include backup of customer data; it is the responsibility of customers to backup any required data.

We manage backups of the cloud infrastructure and systems. We also manage backups of the meta-data used to provide the service, for example the network configuration of your virtual machines.

Backups of meta-data:

- Backups are performed **daily**
- Backup data is stored **offsite**, the offsite location is **between 7 and 15 km** from the location of the data being backed up
- We test the restoration of backup data on **an ad-hoc basis depending on when there has been a significant change in the backup arrangement;** the test conducted is **determined on the basis of the change that triggered the test**
- Access to backup meta-data or archive meta-data **is not** available to you
- We **do not** allow client audits of backup meta-data. We may disclose the results of internal audits as required to third-party auditors.
- Backup data is retained for **24 months**

Maintenance:

- We **do** undertake a regular maintenance programme to ensure the reliability and stability of our cloud resources.
- We **do** undertake a regular maintenance programme to ensure the reliability and stability of our service offerings.

8 Geographic Diversity

It is likely that a service provider may provide services from multiple locations in order to provide resilience of service when adverse events affect one of the locations. This section seeks to understand the locations in which the service provider provides their services from and where they carry out their business activities, as this may indicate the legal jurisdictions that are relevant to their services

- Our service **is** provided via multiple locations
  - Our services are approximately **400** km apart in distance
- Our services are provided from the following locations: **New Zealand**
- We operate offices in the following countries: **New Zealand**
- We have staff in the following countries: **New Zealand**
- We have contractors in the following countries: **France, New Zealand**

9 SLA and Support

Cloud Service Providers may offer premium support packages that are additional to their standard service offering; likewise your contract with them may have special support services just for you. This section sets out the **standard** support mechanisms and service level agreements that apply to services.

- Our standard support hours are **New Zealand Standard Business Hours (08:30 – 17:30, Monday to Friday)**. In the event of an unscheduled outage or incident, we will communicate the details of the issues and expected resolution times via **email** or for customers with Premium Support contacts via **phone.**
- When communicating an issue to us we prefer you to do so via **the web interfaces that we provide.**
- Our standard response time to any support issue raised varies based upon the support package that a customer has subscribed to, for details see: **https://catalystcloud.nz/support/premium-support/**
- In the event of a major incident, we will update our notifications **at least every 2 hours**.
- When communicating with you we will use **the email details provided by you to us.**
- We **do** make incident reports available to our clients after a major incident.
- We **will** shut down or isolate any service offering that is impacting, or will impact, service level agreements.
- We **do not** require service offering specific tools to enable safe service offering shutdown or isolation if needed.
- We operate an **active/active** based service.

Additional disclosures about the service:

- The Terms of Service are available from **https://catalystcloud.nz/about/terms-and-conditions/**
- In the event of a major incident, we will update **https://status.catalystcloud.nz/**
- You must choose and implement an active/active, active/passive or other based service. We support you by supporting the provision of your virtual machines in multiple locations, if desired.

10 Data Transportability

This section identifies how data may be obtained during the service being provided and after the service has ceased and any related costs.

- We **allow** the use of an API to access data during service provisioning and consumption.
- Data **will not** be available to download after we cease supplying service to you.

11 Business Continuity

The service provider should disclose what their own business continuity preparations are, which may include an upstream provider's SLA, redundancy and fail over.

We have designed our services with the following business continuity preparations:

- Each Catalyst Cloud data centre we operate has Internet connectivity provided over diverse fibre cables.
- Each Catalyst Cloud data centre we operate has backup electricity supplies.
- All key components of the service have been designed and deployed in High-Availability configurations such that failure of one component will not jeopardise delivery of the service.
- The Block Storage service, that is used for storage of the disk volumes used by any virtual machines, ensures that three copies of data are stored on different servers distributed across the cloud infrastructure. Failure of an individual server or disk will result in automatic rebuild onto a new server or disk as appropriate.
- The Object Storage service has multiple storage profiles available, including a profile for geo-replication of objects to Catalyst Cloud data centres.
- Customer data including disk volumes can be migrated from one Catalyst Cloud region to another.

12 Data Formats

- All client data **can** be exported at any stage of the service delivery in the following formats:
  - Object Storage Service – objects can be downloaded in their original format using HTTPS.
  - Block Storage Service – disk volumes can be backed up to object storage and downloaded in their raw format using HTTPS.
  - Compute Service – Compute instances can be backed up as a set of raw disk images and can be downloaded using HTTPS.
  - Customer meta-data - meta-data about the customer's virtual private cloud, including networks and compute instances attached to each network, can be retrieved using an HTTPS-based API. The data will be formatted as plain text and structured in a JSON format.
- Our API requires data to be transmitted in the formats defined above.

13 Ownership of Application

- The source code for the **underlying Catalyst Cloud service is** available to license on your systems outside of our service provision under Open Source licences.
- You are the licensee for any software installed into Compute instance.
- It **will** be possible to use your data downloaded from our systems in its native form outside of our service (i.e. your local network) by **creating virtual machines and connecting to disk volumes that have been copied from our service**.

14 Customer Engagement

- We **do** allow the auditing of customer managed **Compute instances** by customers, or their agents.
- We **do not** allow the auditing of our cloud infrastructure and services by customers, except for their **Computer instances**.
- We **do** have an acceptable use policy that is applicable to the services stated in section 5.2. This policy can be found on **https://catalystcloud.nz/about/terms-and-conditions/**
- We **do not** operate a Privacy Policy. (We **do not** manage any privacy related information directly as part of the service). The Catalyst Cloud Terms and Conditions state that the privacy of your data is protected by the New Zealand Privacy Act 2020.

15 Data Breaches

Understanding what will happen when there is a data breach is important.

- If we discover that your data has been lost or compromised, we will **always** notify you as soon as practicable by **email or phone**, unless that notification would compromise a criminal investigation into the breach.
- When we are in possession of evidence of criminal activity associated with the breach (such as evidence of hacker activity) we will **sometimes** notify appropriate law enforcement agencies, depending on **discussions with you about the breach and the lost or compromised data**. We **may** request that you notify law enforcement agencies about the breach.

16 Law Enforcement

When requested by appropriate law enforcement agencies to supply customer related information without a warrant or legal mechanism to compel disclosure:

- It is our usual policy **not to** comply with such requests.

17 Region Specific Disclosures

Please list the countries to which you are becoming a signatory to the CloudCode.

- New Zealand

Appendix A: Cloud Security Alliance STAR Registry Information

The CSA Security, Trust & Assurance Registry (STAR) is a publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with.

Listing on the STAR Registry is a core security activity recognised by the CloudCode and is encouraged for all Cloud Computing providers.

The CSA STAR service is based upon the CSA Governance, Risk and Compliance (GRC) Stack, a collection of four integrated research projects that provide a framework for cloud-specific security controls, assessment, and greater automation and realtime GRC management.

There are two self assessment models inside the STAR program, the Cloud Controls Matrix (CCM) and the Consensus Assessments Initiative Questionnaire (CAIQ, pronounced cake). Service Providers can choose which model to undertake.

The Cloud Controls Matrix (CCM), provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. Providers may choose to submit a report documenting compliance with Cloud Controls Matrix.

The Consensus Assessments Initiative Questionnaire is based upon CCM and provides industry-accepted ways to document which CCM security controls exist in IaaS, PaaS, and SaaS offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Providers may opt to submit a completed CAIQ, this will likely be the easiest option for those who have not already developed a CCM report.

More information on the CSA STAR registry can be found on the Cloud Security Alliance website: https://cloudsecurityalliance.org/star/

18 Schedule 1: New Zealand Specific Content

18.1 S1.1 Data Breach Notification

The Office of the Privacy Commissioner has published r required breach notification guidelines, which can be found at **www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/evaluate**

- The Data Breach Notification we will make in Section 1.15 **will** be made consistent with the required breach notification guidelines issued by the Office of the Privacy Commissioner in New Zealand.
- Where we are able to determine that there has been significant loss or compromise of information, involving sensitive personal information, and there is a risk of serious harm to individuals we **will** notify the Office of the Privacy Commissioner directly.

18.2 S1.2 New Zealand Legislation

- We affirm that we always comply with the Privacy Act 2020, Fair Trading Act 1986, Commerce Act 1986, Copyright (Infringing File Sharing) Amendment Act 2011 and other relevant legislation.