NEW ZEALAND

CLOUDCODE™

CLOUD COMPUTING CODE OF PRACTICE

DISCLOSURE STATEMENT PREPARED BY

Umbrellar Limited

AS AT 04 July 2017

CLOUDCODE™ NEW ZEALAND SIGNATORY
CLOUD COMPUTING CODE OF PRACTICE

CLOUDCODE™ NEW ZEALAND PROVISIONAL SIGNATORY
CLOUD COMPUTING CODE OF PRACTICE

Institute of IT Professionals NEW ZEALAND

1 Introduction

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:

1. Corporate Identity

Company name: .....**Umbrellar Limited**.....

Company Registration Number: .... 9429032313628…....

Trading name: .....**Umbrellar**.....

Physical address: .....**3/78 Apollo Drive, Rosedale, Albany, 0632, Albany**.....

Postal address:..... **3/78 Apollo Drive, Rosedale, Albany, 0632, Albany** .....

Company website:.....**http://www.umbrellar.com**.....

Contact phone number: .....0800 344 493 …….....

Contact email address: .....**info@umbrellar.com**.....

Complaints about our service can be made in the first instance to: . **info@umbrellar.com**

Contact person responsible for these disclosure statements can be contacted via the following email address:

....**david.howden@umbrellar.com**.....

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

- ....**Cloud Servers**…….....as described at www.umbrellar.com

For the purpose of Legal Jurisdiction, the contracted supplier who provides the service to you is a Registered Company registered in ……..**New Zealand**.....

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

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

2. Ownership of Information

We **do not** claim ownership of any data or information uploaded to our service.

Your data and information may traverse or be stored on our upstream provider's networks or systems. In these instances that 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** and **is** used for the purposes of ....**improving service**.....

3. Security

As at the date of application:

- We **are not** listed on the CSA STAR Registry.
- We do not formally meet any security related standards
- We have the following physical security in place at the data centre's hosting your data:
  24/7 Onsite Security, biometric and proximity card only access, CCTV monitoring of facility, early warning smoke detection systems, concrete floors, walls and ceilings
- We have the following digital security in place on the systems hosting your data:
  ……**Firewalls and internal only access available to infrastructure services**.....

4. Data Location

- Our primary systems that host your data are located in
  .....**Auckland, New Zealand** & Christchruch, New Zealand
  .....
- Our Backup/Disaster recovery systems that hold your data are located in
  ..... **Auckland, New Zealand**. & Christchruch, New Zealand.....

5. Data Access and Use

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 via the following formats: .....**any format as uploaded**.....

- At the cessation of our service to you, your data **will** be available to access
  - Access to this data will be granted via …**any method as uploaded**…….....
  - There **will** be additional charges for access to your data after the service has been ceased

Data access by us:

- Deletion of all customer data at the cessation of our service to you takes place

  .....**30 days after the cessation of our service to you**.....
- We use customer data for the following business functions
  - *Systems Monitoring*
- We **do not** access customer data for any other 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.

  ......**Fully comply with local regulations**.....
- We **do not** provide access to customer data to third parties other than law enforcement agencies as set out above.

6. 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.

- Backups are performed ……**daily**…….
- Backups include **system data and statistical data**
- Backup data is stored ……**onsite and or at a secondary NZ based DC where required as part of the procured service.** ……..……..
- We test the restoration of backup data every .....**N/A**.....

  and the test is conducted.....**N/A**.....
- Access to backup data or archive data **is** available via .....**Customer web interface**.....
- Adhoc requests for restoration of customer data will be commenced within ……**4hrs (BH)**…….
- We **do not** allow client audits of backup data.

- Backup data is retained for .**7 or 28 days days depending on purchased product**
- 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.
- Additional information regarding backups:
  It is expected that the customers back up their own data via subscribing to one of our backup products. We maintain backups of system data for which products they procure and statistical data only

7. Geographic Diversity

- Our service **is** provided via multiple locations
- Our services are provided from the following location(s): .....**New Zealand (Auckland & Christchruch)**.
- We operate offices in the following country(s): ..... **New Zealand (Auckland & Christchruch)**.....

8. SLA and Support

This section sets out the **standard** support mechanisms and service level agreements that apply to services.

- Our standard support hours are.....**M-F 8:30am – 18:30pm with OOO for priority incidents.**
- In the event of an unscheduled outage or incident, we will communicate the details of the issues and expected resolution times via ..... **https://www.umbrellar.nz/status/**
- When communicating an issue to us we prefer you to do so via **https://www.umbrellar.nz/status/**
- Our standard response time to any support issue raised is .....1-hour…….....
- In the event of a major incident, we will update our notifications every .....**1**.. hours., **unless stated otherwise**
- When communicating with you we will use .....RSS+email.....
- 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 information regarding SLA and Support:

We classify incidents and therefore the resolution time to issues in the following way

Severity Level	Classification Method	Expected resolution time
Major	**affects more than 70% of clients during business hours**	**4 hours**
critical	**affects more than 50% of clients during business hours**	**4 hours**
minor	**affects less than 10% of clients outside of business hours**	**6 hours**

9. Data Transportability

(please delete the appropriate statement)

- We **do not allow** the use of an API to access data during service provisioning and consumption.

- Data **will** be available to download after we cease supplying service to you
  (if data is available post service cessation, then the following statement will apply)

  Data can be obtained via .....making contact with us.....

- There **may** be additional charges associated with accessing data after your service has ceased.

10. Business Continuity

N/A (We do not disclose continuity procedures) – These can be discussed as part of a customer engagement.

11. Data Formats

- All client data **can** be exported at any stage of the service delivery in the following formats: .....**any as uploaded**.....

- Our API requires data to be transmitted in the following formats .....**N/A**.....

Additional information regarding SLA and Support:

N/A

12. Ownership of Application

- The source code for the applications that you use on our service **is not** available to license on your systems outside of our service provision.
- 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 .....**any method as uploaded**.....

13. Customer Engagement

- We **do not** allow the auditing of our services by customers
- We **do** have an acceptable use policy that is applicable to the services stated in section 5.2.
- We **do** operate a Privacy Policy.

14. Data Breaches

- If we discover that your data has been lost or compromised, we will **always** notify you as soon as practicable by .....**email** , 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. (If “if the criminal activity is within New Zealand jurisdiction. Criminal activity such as hacking attempts occur nearly continuously from all over the globe. While we monitor and block such activity it would be impossible to notify every relevant enforcement agency.

15. 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 **to** comply with such requests.

16. Region specific Disclosures

Please list the countries to which you are becoming a signatory to the CloudCode. (Currently just New Zealand).

- **New Zealand**

Schedule 1:
New Zealand specific Content

S1.1 Data Breach Notification

The Office of the Privacy Commissioner has published voluntary breach notification guidelines, which can be found at **www.privacy.org.nz/privacy-breach-guidelines-2**

- The Data Breach Notification we will make in Section 5.15 **will/** be made consistent with the Voluntary 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 and a risk of harm to individuals we **will also** notify the Office of the Privacy Commissioner directly.

S1.2 New Zealand Legistation

- We affirm that we always comply with the Privacy Act, Fair Trading Act, Commerce Act, Copyright (Infringing File Sharing) Amendment Act 2011 and other relevant legislation.
- We **do/** have a current Fair Trading Act Compliance policy, a copy of which is attached.

S1.3 Fair Trading Compliance Policy (Sample)

A sample Fair Trading Act Compliance Policy can be downloaded from http://nzco.mp/fta