OneNet®

Trusted partner in cloud computing

DISCLOSURE STATEMENT PREPARED BY

OneNet Limited

AS AT   28 August 2017

NEW ZEALAND

CLOUDCODE

CLOUD COMPUTING CODE OF PRACTICE

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: .... **OneNet Limited**

Company Registration Number: **1079274**

Trading name: .... **OneNet Limited**

Physical address: .... **161-163 Jervois Road, Herne Bay, Auckland**

Postal address: .... **P O Box 46068, Herne Bay, Auckland**

Company website: ....**www.onenet.co.nz**

Contact phone number: **09 376 7610**

Contact email address: .... **support@onenet.co.nz**

Complaints about our service can be made in the first instance to. ***complaints@onenet.co.nz***

Contact person responsible for these disclosure statements can be contacted via the following email address: **michael.snowden@onenet.co.nz**

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

• ***Desktop as a Service (DaaS)*** as described at ***http://www.onenet.co.nz/solutions/desktop-as-a-service/***

• ***Infrastructure as a Service (IaaS)*** as described at ***http://www.onenet.co.nz/solutions/infrastructure-as-a-service/***

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

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

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 provider_** and **_is_** used for the purposes of **_improving our service to you._**

3.   Security

As at the date of application:

- We **_are_** listed on the CSA STAR Registry.

- We are currently undergoing the process of acquiring certification against the following security related standard(s): **_ISO27001_**

- We have the following physical security in place at the data centres hosting your data:
  OneNet co-locates its equipment in high-grade Tier 3+ facilities, which includes a photographic recording of all attendees, CCTV monitoring and 24/7 on-site operational management and security staff.

- We have the following digital security in place on the systems hosting your data:
  Dual Firewalls, Intrusion Prevention Systems (IPS), Centrally managed antivirus, Centrally managed Microsoft software updates, SSL/TLS encrypted communications, Access event logging. Email and internet anti-spam and anti-virus protection. Complex password policy, External security audits.

4.   Data Location

- Our primary systems that host your data are located in **_Auckland, New Zealand_**
- Our Backup/Disaster recovery systems that hold your data are located **_Hamilton, 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 **_native format or other format requested by you_**

- At the cessation of our service to you, your data **_will_** be available to access

- Access to this data will be granted via **_your username and password_**

- There **_may 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 *__after seven days, unless mutually agreed otherwise.__*

- We use customer data for the following business functions:
  __We do not use data for any business function__

- 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 *__conform to the edicts of the law or comply with any legal process served on OneNet.__*

- 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 every *__day__*.

- Backups include (tick those that apply)
  ☒ system data
  ☒ client data
  ☐ statistical data
  ☒ operating system data
  ☐ other

- Backup data is stored *__off site__*

- Where backup data is stored offsite, the offsite location is __135km__. km from the location of the data being backed up.

- We test the restoration of backup data *__periodically__* and the test is conducted *__as a full restoration__*

- Access to backup data or archive data *__is__* available via *__a service request__*

- Adhoc requests for restoration of customer data will be commenced within *__4 hours__*

- We *__do__* allow client audits of backup data, costs of which will be carried by *__the client organisation__*

- Backup data is retained for *__4 weeks__*

- 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.

7. Geographic Diversity

- Our service _**is**_ provided via multiple locations

- Our services are approximately. _**135**_..km apart in distance

- Our services are provided from the following locations: _**New Zealand**_.

- We operate offices in the following countries: _**New Zealand**_

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. _**8.00am to 5.00pm**_ (local time unless stated otherwise).

- In the event of an unscheduled outage or incident, we will communicate the details of the issues and expected resolution times via _**OneNet's twitter feed (@OneNetNZ)**_

- When communicating an issue to us we prefer you to do so via _**OneNet's case management (http://support.onenet.co.nz)**_

- Our standard response time to any support issue raised is _**less than two hours**_

- In the event of a major incident, we will update our notifications every _**hour**_

- When communicating with you we will use _**telephone or email**_

- We _**do**_ make incident reports available to our clients after a major incident.

- We _**may**_ shut down or isolate any service offering that is impacting, or will impact, service level agreements.

- We _**may**_ require service offering specific tools to enable safe service offering shutdown or isolation if needed.

- We operate an _**active/passive**_ based service.

9. Data Transportability

- An API is not relevant to the service we offer.

- Data _**will**_ be available to download after we cease supplying service to you

  - Data can be obtained via _**a service request describing the requested data format**_

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

10. Business Continuity

OneNet has redundant firewalls and internet suppliers. OneNet also uses BGP (Border Gateway Protocol to allow for the automatic announcement of new IP Addresses in the case of the primary Internet provider failing. OneNet operate a secondary, DR or HA site, based in Hamilton. Clients are able to optionally subscribe to DR and HA enabled services.

11. Data Formats

- All client data **can** be exported at any stage of the service delivery in the following formats: *native file format*

12. Ownership of Application

- The source code for the application that you use on our service **is** 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 *acquiring the appropriate Microsoft operating system and application software licenses or any relevant Microsoft services.*

13. Customer Engagement

- We **do** 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. This policy can be found at *http://www.onenet.co.nz/acceptableusepolicy/*

- We **do** operate a Privacy Policy. This policy can be found at   *http://www.onenet.co.nz/privacy-statement/*

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 or telephone* 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 **always** notify appropriate law enforcement agencies

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 **not 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 Legislation

- 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 may be found at : ***http://www.onenet.co.nz/fairtradingactcompliancepolicy.***