DISCLOSURE STATEMENT PREPARED BY

Winscribe Inc

AS AT May 1st 2015

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: ..... **Winscribe Inc**

Company Registration Number: **1104328**

Trading name: ..... **Winscribe**

Physical address: ..... **Level 2, 95 Hurstmere Road, Takapuna, Auckland, New Zealand**

Postal address: ..... **Level 2, 95 Hurstmere Road, PO Box 33-178, Takapuna, Auckland, New Zealand**

Company website: ..... **www.winscribe.com & www.winscribe.co.uk**

Contact phone number: ..... **+64 (9) 486 9010**

Contact email address: ..... **s.stuart @winscribe.com**

Complaints about our service can be made in the first instance to. **Simon Stuart, Director of Services via s.stuart@winscribe.com or +64 (9) 486 9010**

Contact person responsible for these disclosure statements can be contacted via the following email address: ***s.stuart@winscribe.com***

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

- **Winscribe SaaS Cloud Services** as described at www. **winscribe.com/speech-technology/licensing-options**

- **Winscribe SaaS Cloud Services** as described at www. **winscribe.co.uk/speech-technology/licensing-options**

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

The governing law of our contract with you is **country-specific as stated in your contract with us.**

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 **operation and administration of the 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 centres hosting your data:
  ASIO T4

- We have the following digital security in place on the systems hosting your data:
  HIPAA compliance and encryption to customer requirements

4. Data Location

- Our primary systems that host your data are located in **New Zealand, the United Kingdom & the United States of America**
- Our Backup/Disaster recovery systems that hold your data are located **as above.**

Additional information about data location: **Data hosting and location is dependent upon the geographical location of the customer. Where necessary we maintain data ONLY in the geographic locations agreed with the customer.**

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 **as stipulated in your contract and license(s).**
- At the cessation of our service to you, your data **will not** available to access.

Data access by us:

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

- We use customer data for the following business functions:
  Provision of the agreed and contracted cloud-based services.

- 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.

  Comply with court-issued warrants and legal due process

- We **do** provide access to customer data to third parties other than law enforcement agencies as set out above.
- Such 3rd party access is provided for the purposes of:
  - Operation of 3rd party software as part of the Winscribe service or
  - Provision of support and maintenance in order for Winscribe to provide continuous operation of the software and software environment.

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 **Night**.

- Backups include (tick those that apply)
  X system data
  X client data
  X statistical data
  X operating system data
  ☐ other *please state.*

- Backup data is stored **offsite**
- Where backup data is stored offsite, the offsite location is **>5**km from the location of the data being backed up

We test the restoration of backup data every **3mths**
and the test is conducted.. **by a test full server restore**

- Access to backup data or archive data **is not available except** via **support request**
- Adhoc requests for restoration of customer data will be commenced within **N/A**
- We **do allow** client audits of backup data, costs of which will be carried by **as agreed in the customer contract**
- Backup data is retained for **7-90 days depending on client requirements**
- 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 provided from the following locations **New Zealand, the United Kingdom & the United States of America**, however services to each individual client are provided from a single location.
- We operate offices in the following countries **New Zealand, Switzerland, the United Kingdom & the United States of America**

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. **9am-5pm** (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 **email**

- When communicating an issue to us we prefer you to do so via **email to support@winscribe.com**
- Our standard response time to any support issue raised is **24hrs or as specified in the customer support contract**
- In the event of a major incident, we will update our notifications every **1** hours.
- When communicating with you we will use **email and phone contacts provided**
- We **do** make incident reports available to our clients after a major incident.
- We **will not** shut down or isolate any service offering that is impacting, or will impact, service level agreements, except with customer agreement.
- We **do not** require service offering specific tools to enable safe service offering shutdown or isolation if needed.
- We operate an **other** based service.
  If 'other" **we provide an enterprise-grade customer-segregated service**

Additional information about SLA's and support:

Click here to enter text .

9. Data Transportability

- We **do not** 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

10. Business Continuity

Our cloud service is provided using multiple redundant servers which run on a highly-available VM infrastructure, itself covered by offsite replication in the event of a disaster affecting the prime site.

11. Data Formats

- All client data **cannot** be exported at any stage of the service delivery in the following formats: ***N/A***
- Our API requires data to be transmitted in the following formats ***N/A***

Additional information can be entered here regarding portability and interoperability features:
Client data can be migrated according to the client's requirements.

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 **installing the appropriate site-licensed application.**

13. Customer Engagement

- We **do allow** the auditing of our services by customers
- We **do not** have an acceptable use policy that is applicable to the services stated in section 5.2. This policy can be found at ***N/A***
- We **do** operate a Privacy Policy. This policy can be found at **http://www.winscribe.com/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 and 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 **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** 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 not** have a current Fair Trading Act Compliance policy.

S1.3 Fair Trading Compliance Policy (Sample)

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