SilkRoad

DISCLOSURE STATEMENT PREPARED BY

SilkRoad

AS AT 2 May 2016

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: ..... **SilkRoad technology NZ Ltd**

Company Registration Number: **2437043**

Trading name: ..... **SilkRoad**

Physical address: ..... ***Level 17 West Plaza Building Corner Albert & Customs Street***

Postal address: ..... **P.O. Box 4006 Auckland 1010**

Company website: ..... **www.silkroad.com**

Contact phone number: ..... **+64 9 913 4656**

Contact email address: ..... **fanna.share@silkroad.com**

Complaints about our service can be made in the first instance to. **Fanna Share**

Contact person responsible for these disclosure statements can be contacted via the following email address: ***fanna.share@silkroad.com***

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

- ***All Modules*** as described at www. **www.silkroad.com**
- *Product type/name.* as described at www. *Enter URL.*
- *Product type/name.* as described at www. *Enter URL.*
- *Product type/name.* as described at www. *Enter URL.*

For the purpose of Legal Jurisdiction, the contracted supplier who provides the service to you is a ***Globally*** registered in **USA**

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

The disclosure statements that follow have been ***Assessed externally*** by **Grant Thornton LLP**

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 **client** and ***is not*** used.

3. Security

As at the date of application:

- We **are not** listed on the CSA STAR Registry.

(delete one of the following statements)

- We formally meet the following security related standards: **SOC2** Type II Report, which have been ***Assessed externally*** by **Grant-Thornton, LLC**
    - We have the following physical security in place at the data centers hosting your data: **Secure, unmarked entrance to building. 24/7 manned security guards, two factor authentication for data center entry. Man-trap. Surveillance cameras throughout the data center. Locked cages for SilkRoad equipment. Fire detection and prevention. Separate environmental controls. Redundant power, Uninterruptible Power Supplies, and Diesel Generators. Redundant Internet Service Providers.**
- We have the following digital security in place on the systems hosting your data: **Firewalls, Network Based Intrusion Prevention systems, Load Balancers that provide network address translation (natting) that hide the true IP address of the servers. System redundancy. DMZ isolation of databases. Security Incident Event Management System. Application monitoring systems. Anti-virus/anti-malware software installed on all servers.**

4. Data Location

- Our primary systems that host your data are located in **North Carolina USA or Alberta Canada**
- Our Backup/Disaster recovery systems that hold your data are located **Norcross Georgia USA and Toronto, Ontario Canada**

Additional information about data location: **Clients has the option to which datacenter hosts the data. Data is not shared between the two.**

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 **Data can be extracted via reports in various formats (CSV, XML, PDF or Word files) Full SQL backups can be requested during contract for a nominal fee.**
- At the cessation of our service to you, your data **will** be available to access

(if answer above is "will be available" please complete the following statements, otherwise delete)

- Access to this data will be granted via **delivery of data via SFTP or encrypted Digital Media**

- There **will not** 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 ***90 days after verification or receipt of delivery of returned data, unless otherwise contracted***

- We use customer data for the following business functions:
  Not used at all
  Click here to enter text.
  Click here to enter text.

- We **do not** access customer data for any other purpose *please outline if you do*
- We **do not** use customer data in order to generate revenue other than through provision of the service. *please outline if you do*

Data access by others:

- If we are approached by law enforcement agencies it is our policy to.

  Immediately notify the client so that they may have an opportunity to pursue any legal remedies prior to SilkRoad granting access

- 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 (incremental) week (full)**.

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

- Backup data is stored **Offsite**

- Where backup data is stored offsite, the offsite location is ***150***. km from the location of the data being backed up.

  We test the restoration of backup tapes annually as part of SilkRoad's Disaster Recovery Test.. ***sample tests***

- Access to backup data or archive data **is not** available via *click here to state method.*

- Adhoc requests for restoration of customer data will be commenced within **8 hours**
- We ***do not*** allow client audits of backup data
- Backup data is retained for ***9 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 not** provided via multiple locations
  (if the service is provided via multiple locations, the following disclosures should be made, if the opposite is true both these statements can be deleted)
  - Our services are approximately. *click here to state distance.*..km apart in distance

    Or
  - Our services are provided via both onshore and offshore locations

- Our services are provided from the following locations: **Winston-Salem, NC, USA or Edmonton, Alberta, Canada**.
- We operate offices in the following countries: ***New Zealand, Australia, United States, Canada, Japan, Philippines, Germany, United Kingdom and Denmark***.

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. **02:00 to 23:00** (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 ***Phone or email***

- When communicating an issue to us we prefer you to do so via ***Phone or email***
- Our standard response time to any support issue raised is ***Severity 1 – 30 minutes Severity 2 – 2 hours Severity 3 – 8 hours Severity 4 – 24 hours***
- In the event of a major incident, we will update our notifications every ***1*** hours.)
- When communicating with you we will use .. ***Salesforce.com***
  (e.g. details provided by customer on application / email)
- 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.
- 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" *click here to state.*

Additional information about SLA's and support:

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

Click here to enter text .

9. Data Transportability

(please delete the appropriate statement)

- 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
  (if data is available post service cessation, then the following statement will apply)

  Data can be obtained via ***Secured return of all data to client***
- There **will not** be additional charges associated with accessing data after your service has ceased.

10. Business Continuity

SilkRoad has a documented Business Continuity Plan and a Disaster Recovery plan to cover most contingencies regarding the loss availability. Redundancy is in place for all systems within the datacentres. In the event of the total loss of a datacentre, operations would be restored to a disaster recovery location, with the Recovery Time Objective being five (5) business days.

11. Data Formats

- All client data **can** be exported at any stage of the service delivery in the following formats: ***XML or CSV***

- Our API requires data to be transmitted in the following formats ***XML***

Additional information can be entered here regarding portability and interoperability features: *Click here to enter text .*

12. Ownership of Application

- The source code for the application that you use on our service ***is not*** available to license on your systems outside of our service provision.
- It **will not** be possible to use your data downloaded from our systems in its native form outside of our service (i.e. your local network) by *state details of how the application can be run outside of the service providers systems .*

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. This policy can be found at ***Attached***
- We **do** operate a Privacy Policy. This policy can be found at **Attached**

14. Data Breaches

- If we discover that your data has been lost or compromised, we will ***always*** notify you as soon as practicable by **phone and email** unless that notification would compromise a criminal investigation into the breach. (If "sometimes", *please state conditions*
- 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. (If "sometimes", *please state conditions*

15. Law Enforcement

When requested by appropriate law enforcement agencies to supply customer related information without a warrant or legal mechanism to compel disclosure:
(please delete the appropriate statement)

- 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 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