NEW ZEALAND CLOUDCODE™

CLOUD COMPUTING CODE OF PRACTICE

Version 2.0 (July 2013)

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

Table of contents

1 Introduction

Cloud Computing can offer significant advantages to businesses and individuals who venture into "the cloud" in terms of cost, flexibility, scalability and convenience. But it is not without risk.

Users of Cloud products and services entrust their important business and personal data to Cloud Service Providers and have the right to know how trustworthy their provider, and their provider's products and services, really are. The Cloud is about *trust*, and the CloudCode helps users make informed decisions.

Signatories to the CloudCode take their responsibilities seriously and make two key commitments:

1. **They won't say an offering is "Cloud Computing" unless it really is** (ie. no "Cloudwashing"). There are specific and significant benefits from genuine Cloud products or services but unfortunately some unscrupulous providers try to pass non-Cloud products or services off as Cloud Computing.
2. **They will disclose important details about their Cloud products and services** - upfront - to allow potential customers to make informed decisions. No surprises, no hiding behind sales pitches, and no obfuscation. Just the facts. And to be sure, the CloudCode sets these disclosures out in detail.

The Cloud Computing Code of Practice ("CloudCode") gives professional and responsible cloud service providers the opportunity to benchmark and demonstrate their practices, processes and ethics via a recognised third party to build trust with prospective customers. The CloudCode was developed by, and is now operated by, the *Institute of IT Professionals NZ*, the independent professional body of the IT industry.

The CloudCode was developed with the input of over 250 cloud providers, users, individuals and other stakeholders and was funded by a group of Cloud providers keen to protect the integrity of this important future-focused sector.

Major Contributors

Equinox IT, Gen-i, OneNet, Webdrive, Xero, Institute of IT Professionals NZ Inc.

Other Contributors

Salesforce.com, Google, EOSS Online, InternetNZ, NZRise, Systems Advisory Services.

Institute of IT Professionals NEW ZEALAND

The CloudCode was also developed with assistance and input from the Cloud Security Alliance (CSA) and Office of the New Zealand Privacy Commissioner.

1.1 Core Principles of the Code

The following are the Core Principles for the development of the CloudCode. These Core Principles will continue to apply during subsequent development:

- **Not reinvent the wheel**
  Where possible, the Cloud Computing Code of Practice leverages existing work in New Zealand and abroad and give clear preference to established prior work over creation.
- **Consistency with global practice and structure**
  A core part of this initiative is researching approaches taken to addressing the core issues in all jurisdictions, to ensure the Code is consistent with practices worldwide.
- **Research based non-arbitrary approach**
  The CloudCode is developed based on demonstrable good practice and decisions taken based on sound research-based principles.
- **Facilitation of development with wide consultation**
  The role of the Institute and the project team is to facilitate the development of the code in consultation with as broad a range of stakeholders as possible and practical.
- **Preference for consensus based result**
  The project team works towards a consensus view in terms of the structure and content of the Code. While consensus does not mean unanimous, the intention is to ensure the wide support of a broad range of stakeholders.
- **Clear separation between governance of process and development of the CloudCode**
  The steering group govern the process, ensuring the principles are adhered to and always testing the evidence based approach, however do not guide or influence the final result and Code.
- **Compliance and Assessment**
  It is not the intention of the CloudCode to place undue or unnecessary compliance costs or processes on those who may wish to adhere to the Code, over and above what is necessary for the integrity of the code.

1.2 Aims of the Code

- Improve the standard of services being provided by the Cloud Computing Industry;
- Set a standard of disclosure within the industry;
- Create openness between providers and customers on data protection, sovereignty and privacy;
- Strengthen the integrity of Cloud Computing in countries that adopt the Code.

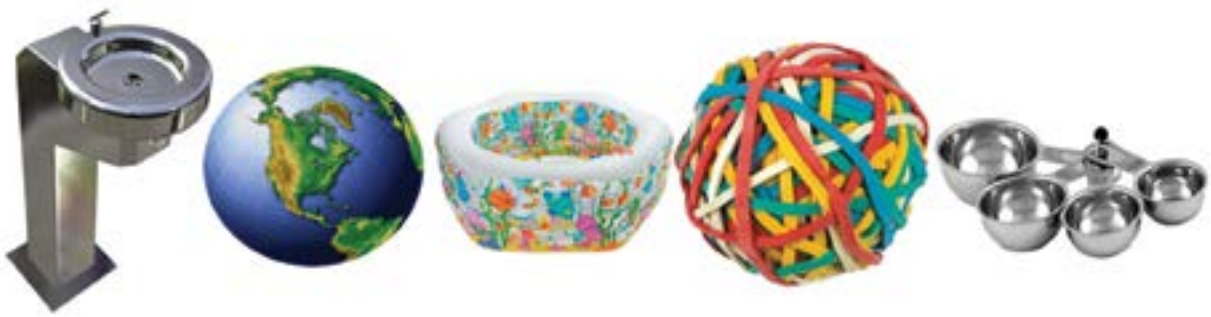
1.3 Changes to the CloudCode: Version 2

Version 2 of the CloudCode incorporates the following:

- An overhaul of the Security section. For example, listing on the CSA Star Registry is now optional;
- Inclusion of Registry details, including becoming a Signatory and use of the CloudCode branding;
- Outline of Disputes and Complaints procedure;
- Structural changes to prepare for international adoption of the CloudCode;
- Other minor wording and structural changes throughout the document;

2 Defining Cloud Computing

5 Essential Characteristics of Cloud Computing



On-demand self-service | Ubiquitous network access | Location transparent resource pooling | Rapid elasticity | Measured service with pay per use

Source: http://aka.ms/532

Cloud Computing has many definitions worldwide and certainly means many different things to many different people. The National Institute of Science and Technology (NIST) have created a definition, which is the most adapted definition in use today. NIST identify five essential characteristics for cloud computing as illustrated above.

For the purpose of this code of practice we have simplified the NIST definition to ensure a simple definition that is easily understood,while formally supporting the full NIST definition as the authoritative definition of Cloud Computing.

Full NIST Definition: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

2.1 What is Cloud computing?

For the purpose of the CloudCode, Cloud Computing is defined as:

> *"On-demand scalable resources such as networks, servers and applications which are provided as a service, are accessible by the end user and can be rapidly provisioned and released with minimal effort or service provider interaction."*

This might include Software-as-a-Service, Infrastructure-as-a-Service, Platform-as-a-Service, or any variant that fits within this definition, and includes both public and private Cloud implementations.

3 Application and Approach

3.1 CloudCode relates to Cloud Provider and their Products and Services

Cloud Service Providers are signatories to the CloudCode. Each provider produces a set of disclosures that meet the requirements of Section 5 of this document for some or all of their products or services. To be a Full Signatory, all products or services marketed implicitly or explicitly as "Cloud Computing" must be covered by at least one Disclosure Document.

Providers with products or services that meet the requirements of Section 4.1 may state that they are a CloudCode Signatory only once their disclosures have been independently confirmed by the CloudCode team and they appear on the CloudCode Register (see below).

Providers who have not yet produced Disclosure Documents for all of their Cloud products or services may be granted Provisional Signatory status until such time as the remaining Disclosure Documents have been completed and confirmed by the CloudCode team.

3.2 Who does the CloudCode apply to?

The CloudCode applies to businesses who offer remotely hosted IT services of any type, either within a country that has adopted the CloudCode or from a country that has adopted the CloudCode, that meet the definition of Cloud Computing as outlined in Section 2.1 of this document.

Products and services which meet the definition in spirit and are generally considered a Cloud offering, but are precluded due to an arbitrary matter related to the definition, will be considered by the CloudCode team on a case by case basis.

The CloudCode is a voluntary code of practice and by becoming a signatory, a service provider represents to the public that they comply with the CloudCode's requirements.

The CloudCode does not in any way place legal obligations on signatories to the Code, however non compliance with the code by a signatory could result in liability under general law (e.g. for misleading and deceptive conduct, an offence under fair trading legislation in most countries).

Continues overleaf...

4 CloudCode Signatories

4.1 Signatory Requirements

The CloudCode is a voluntary code of practice. Signatories to the CloudCode must:

1. Disclose information about their Cloud Products and Services:

1. Produce one or more Disclosure Documents pursuant to Section 5 of the CloudCode and covering all offerings marketed explicitly or implicitly as "Cloud" products or services; *(See Provisional below)*
2. In the case of consultants or others providing independent Cloud-related advice rather than Cloud products or services (excluding those who act as an agent for a Cloud provider), recommend to their clients that they should consider whether or not Cloud providers are signatories to the CloudCode;
3. Comply with their Disclosures at all times and ensure that all products and services covered by Disclosures are provided in accordance with their relevant Disclosures;
4. Act in accordance with the CloudCode's disclosure statements;

2. Notify changes to these Disclosures:

5. Advise clients within 28 days of a change to the disclosures which materially affect the way a product or service is delivered to a client;
6. Produce a Disclosure Document and submit it for review immediately on release of a new Cloud-related Product or Service that is not covered by another Disclosure Document; *(If a Disclosure Document has not been produced and reviewed within 90 days of the release of a new Cloud-based Product or Service, the Signatory will be considered in breach of the clause)*

3. Publicise these Disclosures:

7. Provide a link to their disclosure statements on their publicly available website;
8. Promote the Code on their website via the Signatory logo linked to the CloudCode website;

4. Not "Cloud-wash":

9. NOT market any product or service as a "Cloud" product or service unless it meets the Cloud Computing definition in Section 2.1 (ie no "Cloud-washing"); *Where a product or service meets the spirit of the definition but is excluded on a technicality, the CloudCode team may, at their sole discretion, confirm in writing that it still acceptably meets the definition.*

5. Participate in the CloudCode

10. Undertake the review of Disclosure Documents process as outlined by the CloudCode team;
11. Participate in the Complaint Resolution process outlined in Section 6 if a complaint is received;
12. Be registered on the publicly available ***Register of CloudCode Signatories***; *and*
13. Pay any fees for assessment and listing as outlined from time to time on the CloudCode site.

4.2 Provisional Signatories

Providers wishing to become Signatories, but who have not yet produced Disclosure Documents for all of their Cloud related Products or Services, may become Provisional Signatories if they:

1. Meet all of the requirements in Section 4.1 above, other than Clause 1;
2. Have produced and had reviewed at least one Disclosure Document related to a Cloud related Product or Service they offer;
3. Intend to produce (and have reviewed) Disclosure Documents for all of their Cloud related products or services within a reasonable time.

4.3 Register of CloudCode Signatories and Use of Logos

CloudCode Signatories will appear on the public **Register of CloudCode Signatories** once their Disclosure Documents have been reviewed and found to meet the disclosure requirements of the CloudCode. This process is outlined on the CloudCode website.

Once listed on the Register, Signatories are authorised to use the CloudCode Signatory or Provisional Signatory logos on their websites, marketing materials, tender and quote documents and elsewhere. When used electronically (eg on a website or emailed document) the logo must link back to the CloudCode website.

Signatories may state that Cloud-related products or services which are covered by one or more reviewed Disclosure Documents are compliant with the disclosure requirements of the CloudCode.

The CloudCode team will release specific wording which can be used in conjunction with the logos. Promotion of the Code is restricted to this wording to ensure consistency and clarity in terms, and providing uniformity in the way the Code is promoted to the public. Other terms of use for the logos are available from the CloudCode team.

4.4 Fees

CloudCode signatories must pay an assessment and annual subscription fee to cover the costs of operating the CloudCode and Register of CloudCode Signatories.

Fees will reflect the cost of operating the CloudCode and will be published on the CloudCode website. Any fees changes will be notified on the CloudCode website at least 90 days before they come into effect.

A provider will be withdrawn as a Signatory following non-payment of applicable fees, if payment is still outstanding following the expiration of a *14-day Notice of Intention to Lapse Signatory Status*.

4.5 Withdrawal of a Signatory

A Signatory who wishes to voluntarily withdraw from this CloudCode must:

- Provide at least 60 days notice of their intention to withdraw to the CloudCode team, in writing in the manner prescribed on the CloudCode website;
- Advise existing users of their products or services that were covered by the CloudCode of their intention to withdraw from the CloudCode, at least 45 days prior to their withdrawal.

The requirements above shall not apply if the CloudCode team has advised that the CloudCode and CloudCode Register has ceased operating.

All providers who are removed from the Register of CloudCode Signatories, whether due to (1) voluntary withdrawal; (2) withdrawal due to non-payment of CloudCode fees; or (3) withdrawal as a result of a complaint or dispute (as outlined in Section 6), must:

- Remove all logos, marks and references to their being a signatory to the CloudCode from all marketing material and websites on or before the date of their withdrawal;
- No longer promote any of their products or services as being compliant with the disclosure requirements of the CloudCode.

5 Code of Practice Disclosures

5.1 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:

5.2 Corporate Identity

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

Company name: .....

Company Registration Number: .....

Trading name: .....

Physical address: .....

Postal address: .....

Company website: .....

Contact phone number: .....

Contact email address: .....

Complaints about our service can be made in the first instance to: .....

(contact details of the relevant contact point) .....

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

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

- .....as described at www.....
- .....as described at www.....
- .....as described at www.....
- .....as described at www.....
- For the purpose of Legal Jurisdiction, the contracted supplier who provides the service to you is a [company] registered in .....(state country)
- The governing law of our contract with you is .....(state jurisdiction)
- The disclosure statements that follow have been Self Assessed / Assessed externally

  by .....(state auditing organisation's name)

5.3 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 / 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 **client / service provider/ upstream provider.**
- Metadata and other statistical information, such as anonymised data generated as a result of the use of our service, is owned by **client / service provider / other** and **is / may be** used for the purposes of .....

5.4 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 date of application:

- We **are/are not** listed on the CSA STAR Registry.
- We formally meet the following security related standards: .....(state standards held) at level……..(state levels held) which have been **self assessed / externally assessed or audited** by ……(state name of assessor).
  or:
  We are currently undergoing the process of acquiring certification against the following security related standard(s)..... (state standard).
- We have the following physical security in place at the data centres hosting your data: .... (please state)
- We have the following digital security in place on the systems hosting your data: .... (please state)

5.5 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.....(Please state country and the state if applicable)
- Our Backup/Disaster recovery systems that hold your data are located in ....(Please state country and the state if applicable)

Additional disclosures may be provided here by the service provider such as the location of specific data centres and backups.

5.6 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 via the following formats .....
- At the cessation of our service to you, your data **will/will not** be available to access
    - (if answer above is "will be available") Access to this data will be granted via ....(state method)
    - There **will / 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 .....(state timeframe)
- We use customer data for the following business functions
    - List item 1
    - List item 2
    - List item 3
- We **do/do not** access customer data for any other purpose (please outline if you do)
- We **do/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..... .....(state policy)
- We **do/do not** provide access to customer data to third parties other than law enforcement agencies as set out above.

5.7 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.

- Backups are performed every ..... (how often: e.g. hourly, daily, weekly, monthly)
- Backups include system data/client data/statistical data/Operating System data/other
- Backup data is stored ..... (onsite, or offsite, relative to the location of the data being backed up)
- Where backup data is stored offsite, the offsite location is ..... km (distance in kilometres) from the location of the data being backed up

- We test the restoration of backup data every .....(how often) and the test is conducted.....(state how restoration is tested, i.e. sample tests, full restore compare etc)
- Access to backup data or archive data **is / is not** available via .....(method)
- Adhoc requests for restoration of customer data will be commenced within …….. (elapsed time from request)
- We **do / do not** allow client audits of backup data, costs of which will be carried by.....
- Backup data is retained for .....(state period)
- We **do/do not** undertake a regular maintenance programme to ensure the reliability and stability of our cloud resources
- We **do/do not** undertake a regular maintenance programme to ensure the reliability and stability of our service offerings.

Note: Backups should not be limited to 'customer data'. They should also include any data or configuration items which form 'the service' being provided by the cloud service provider, including (where applicable), but not limited to: customer data, configuration settings, files, documents, operating systems, applications, permissions. The Backup and subsequent restoration capability should be comprehensive enough to enable the Cloud Service Provider to fully restore-to-operation the 'service' and any customer data.

5.8 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 / is not** provided via multiple locations *(if the service is provided via multiple locations, the following disclosures should be made)*
    - Our services are approximately.....km apart in distance

    Or

    - Our services are provided via both onshore and offshore locations
- Our services are provided from the following locations: ..... *(stating the countries where services are being provided from)*
- We operate offices in the following countries: .....

5.9 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.....(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 .....

- When communicating an issue to us we prefer you to do so via .....
- Our standard response time to any support issue raised is .....
- In the event of a major incident, we will update our notifications every ..... hours.
- When communicating with you we will use .....(e.g. details provided by customer on application)
- We **do / do not** make incident reports available to our clients after a major incident.
- We **will /will not** shut down or isolate any service offering that is impacting, or will impact, service level agreements.
- We **do / do not** require service offering specific tools to enable safe service offering shutdown or isolation if needed.
- We operate an **active/active, active/passive or other** ..... (please state) based service.

Additional "plain English" statements may be offered under this heading with regards to the service providers service and SLAs including clarification of the supplier's position with regard to its support and SLA provisions contained in its customer contracts.

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

  or: An API is not relevant to the service we offer.
- Data **will / 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 .....
- There **will / may / will not** be additional charges associated with accessing data after your service has ceased.

5.11 Business Continuity

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

5.12 Data Formats

- All client data **can / cannot** be exported at any stage of the service delivery in the following formats: ..... (we suggest a minimum of CSV or XML)
- Our API requires data to be transmitted in the following formats .....
  Additional statements may be offered under this heading with regards to portability and interoperability features that the service provider may have

5.13 Ownership of Application

- The source code for the applications that you use on our service **is/is not** available to license on your systems outside of our service provision.
- It **will / 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 provider's systems)

5.14 Customer Engagement

- We **do/do not** allow the auditing of our services by customers
- We **do/do not** have an acceptable use policy that is applicable to the services stated in section 5.2. This policy can be found at .....(state URL of AUP)
- We **do/do not** operate a Privacy Policy. This policy can be found at .....

5.15 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/sometimes** notify you as soon as practicable by .....(state means), unless that notification would compromise a criminal investigation into the breach. (If "sometimes", please state conditions for notification)

- When we are in possession of evidence of criminal activity associated with the breach (such as evidence of hacker activity) we will **always/sometimes** notify appropriate law enforcement agencies. (If "sometimes", please state conditions for notification)

5.16 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 **to / not to** comply with such requests. *or*

- It is our usual policy to disclose only the following information ..... (e.g. metadata, or names and addresses only)

5.17 Region specific Disclosures

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

Please append any disclosures contained in the country-specific schedule(s) for these countries here.

6 Complaints

The CloudCode complaints process is for consumers, companies and service providers who believe that a statement made by a CloudCode Signatory in their Disclosure Document is untrue or not accurate.

The Register acts on complaints received, however the CloudCode Register itself may act as a Complainant if the CloudCode team suspects that a statement in a Disclosure Document is inaccurate.

This process is **not** intended for the following situations:

- Complaints about a service or product;
- Complaints about support, lack of service or issues surrounding restoration of service;
- Complaints regarding breaches of local laws and regulations that exist;
- Issues surrounding payment, pricing or collection of payments for services;
- Complaints about misleading product information or advertising, other than where the alleged misleading information amounts to a breach of the CloudCode requirements.

Any complaints of the above nature received will be referred back to the complainant.

6.2 How to make a Complaint

If you believe that a CloudCode Signatory has made a false or inaccurate claim with respect to a disclosure statement, you must submit your complaint in writing.

The complaint must include the following details:

- Details of the CloudCode Signatory you are making a complaint against;
- Details of the disclosure you are challenging;
- The reasons why you are challenging the disclosure;
- Any supporting documentation that relates to the matter;
- Your contact details including address, phone and email address.

The more information provided in the complaint the faster the CloudCode team will be able to start the process to resolve the issue. The contact details of the CloudCode Complaint Resolution Service are contained on the CloudCode website.

6.3 Complaints Resolution Process

When a complaint is received, the complainant will be acknowledged by email.

The CloudCode investigation team will initiate an investigation into the matter via the following process:

1. Contact will be made with the Signatory concerned, who in the first instance will be given an opportunity to response to the complaint;
2. The investigative team will seek further information as appropriate and may convene a panel of independent experts. The complaint, response and further information will be considered by the investigation team and a draft report with findings and the proposed resolution will be prepared and sent to all parties;
3. The complainant and the respondent will be given 14 days to respond to the report, including

having the opportunity to correct any inaccuracies in the report;

4. Following further consideration of any responses, a final report will be issued.
5. The complainant and the respondent may appeal the decision within 14 days via a documented Appeals Process provided by the relevant country's CloudCode team.
6. If no Appeal is lodged within 14 days, or an Appeal fails, the resolution outlined in the report will be enacted.

An investigation may take anywhere from a day to several months depending on the nature of the complaint.

6.4 Possible Outcomes of a Complaint

Following an investigation of a complaint, one or more of the following outcomes will be contained in the final report:

1. That no further action is required;
2. That a Signatory must update a disclosure statement or correct an anomaly;
3. A referral of the matter to be directed to a relevant local authority;
4. That the Signatory be withdrawn from the Register of CloudCode Signatories.

The Final Report may direct that the report, outcomes or resolution remain confidential or be released publicly. If the resolution is released publicly, the respondent may or may not be identified.

7 Maintaining the CloudCode

The CloudCode will be reviewed on a regular cycle. It is expected that minor changes are made every six months, with an annual review conducted to ensure it remains relevant and up-to-date with changes in Cloud technology and application.

All changes to the requirements of the CloudCode will be widely consulted and will only proceed with the support of the Cloud Computing industry.

Consultations will be advised via:

1. The CloudCode website;
2. Directly to CloudCode Signatories;
3. Via a mailing list maintained to inform stakeholders about CloudCode activities.

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/

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/will not** 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 / will not** 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/do not** have a current Fair Trading Act Compliance policy, a c 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