New Zealand Cloud Code of Practice

Draft Structure and Approach *- December 2011 v0.8*

Contents

1. Introduction 4

1.1 Core Principles of the Code 5

1.2 Aims of the Code 5

2. Defining Cloud 6

2.1 What is Cloud computing 6

3. Application 7

3.1 Who does this Code of Practice apply to? 7

4. Approach 7

4.1 Cloud Code of Practice to relate to Provider's Products or Services 7

4.2 Compliance with the Code of Practice 7

5. Structure 9

5.1 Disclosure 9

5.2 Additional Modules 11

5.3 Customer Engagement 12

5.4 Assessment 12

5.5 Recognition of Compliance to this code. 12

5.6 Maintenance of this code 12

6. Reference Material 13

For the purpose of providing a draft structure, this document contains various types of text, some annotations, some text is suggestive and some is descriptive.

ANNOTATIONS will display as follows – note this text will be removed prior to the final draft of the code of practice being released.

Text in a box like this is information not intended to be in the final draft of the CoP

SUGGESTED WORDING will display as follows:

Heading

Text here with suggested wording for this section

A DESCRIPTIVE SECTION will display as follows:

Heading

Text here with description of the type of information that could be included – the specific content will need to be consulted on, therefore this is only an illustration of what may be included

1. Introduction

The purpose of the New Zealand Cloud Computing Code of Practice ("The Code") is to enable professional cloud service providers to benchmark and demonstrate their practices, processes and ethics via a recognised third party to build trust with prospective customers. This can be achieved by service providers or suppliers meeting The Code, and having recognition made via a distinguished mark, or entry into a register of compliant cloud providers.

The Code will assist end users by allowing them to make informed decisions based on the disclosure of practices of the service provider, enabling the end users to gain comfort with the service provider's ability to meet end users requirements.

The Code will also build trust within the Cloud Service Industry, providing a trusted format to which both suppliers and customers can depend upon.

Additionally service providers may wish to further their level of compliance by subscribing to an additional module of compliance. These modules provide a greater level of compliance in the areas of Security, Data Transportability, Service dependencies, and Business continuity, HR Procedures, Data Formats and Jurisdictions.

The code recognises the valuable financial support that the following organisations have made in order to have the Code of Practice developed, along with the participation of over 150 individuals from both around New Zealand and off shore.

Equinox, Gen-i, OneNet, Webdrive, Xero, Salesforce.com, Google, EOSS Online Ltd, InternetNZ, NZRise, Systems Advisory Services and the NZ Computer Society (NZCS).

1.1 Core Principles of the Code

The Core Principles for the development of the Cloud Code of Practice as set out in the Terms of Reference V1.0 are:

- **Not Re-inventing the Wheel**
  Where possible, the NZ Cloud Computing Code of Practice should leverage 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 overseas jurisdictions, to ensure the result is consistent with practices in other countries.
- **Research based on –arbitrary approach**
  The recommendations and resultant Code will be developed based on demonstrable good practice and decisions taken based on sound research-based principles.
- **Facilitation of Development with Wide consultation**
  the role of NZCS 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 will work towards a consensus view in terms of the structure and content of the Code. While consensus does not mean unanimous, the intention is to gain the wide support of a broad range of stakeholders.
- **Clear separation between governance of process and development of Code**
  The steering group will govern the process, ensure the principles are adhered to and test the evidence based approach, however will not guide or influence the final result and code.
- **Compliance and Assessment**
  It is not the intention of the exercise to place undue or unnecessary compliance costs or processes on those that may wish to adhere to the code once developed, over and above what is necessary for the integrity of the code.

1.2 Aims of the Code

The Code aims to:

- Improve the standard of services being provided by New Zealand Business in the Cloud Computing Industry
- Set a standard of disclosure within the industry
- Create openness between supplier s and customers with regards to data protection, sovereignty and privacy.
- To strengthen the integrity of Cloud Computing in New Zealand.

2. Defining Cloud

The definition of Cloud computing for the purpose of this document was widely consulted on. The majority of those consulted preferred to use a variation on the NIST definition. However many also supported maintaining the standard definition and given the core principle of not reinventing the wheel it is being proposed that a simplified modification of the NIST definition is used as the headline definition with reference to the full formal NIST definition as the authoritative definition.

5 Essential Characteristics of Cloud Computing

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 5 essential characteristics for cloud computing as illustrated above.

For the purpose of this code of practice we have also adapted the NIST Definition to ensure a simple definition that is easily measured against however formally support 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 New Zealand Cloud Code of Practice, Cloud computing is to be defined as :

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

3. Application

3.1 Who does this Code of Practice apply to?

The New Zealand Cloud Computing Code of Practice applies to businesses who operate within New Zealand that offer remotely hosted IT services of any type that meet the definition of Cloud Computing as outlined above.

4. Approach

The New Zealand Cloud Computing Code of Practice is an Industry led voluntary code which organisations can subscribe to in order to promote their standards of operations and processes are in accordance with acceptable levels as provided for in this code. As highlighted in the Structure and Approach Survey Document, 73% of survey respondents preferred a disclosure based code. The majority of respondents also supported some form of assessment, whether it be random, complaints based or the basis of compliance under this code.

4.1 Cloud Code of Practice to relate to Provider's Products or Services

The Code will relate to specific products or services offered by specific providers. This means:

- Providers whose offerings meet the test of compliance may state that they are compliant with the NZ CloudCode. HOWEVER they must state specifically what product or service offerings comply.
- Providers may only achieve compliance if *all* of their "Cloud" marketed offerings are compliant with the Code. Ie They cannot claim compliance if they are offering "Cloud" products or services that don't meet the requirements of the Code.
- Providers may not implicitly or explicitly claim that any other non-Cloud offerings they provide are compliant with the Code.

4.2 Compliance with the Code of Practice

The Code is a voluntary code. Those who are formally compliant to this code will:

- Comply with the code's minimum level of security requirements (based on existing standards and models)
- Adhere to the code's good practice guidelines
- Provide a full set of stated disclosures to all clients upfront (whether a specific request for such is made or not)
- Update information as disclosed to their clients prior to a change being made or if this is not possible, within 28 days at most of such a change to disclosures
- Maintain a professional service to their clients
- Provide a link to their disclosure statements on their publicly available website
- Promote the Cloud Code of Practice on their site via a link to the NZ Cloud Code website
- NOT engage in conduct that is misleading or deceptive or misrepresent the benefits or features of their product or service

- NOT market a product or service as a “Cloud” product or service unless it meets the cloud definition as above
- NOT market a product or service as a “Cloud” product unless it meets all base requirements of the Code

Organisations who become compliant to this code may also choose to subscribe to additional modules of the code, providing more detail and protection for the end users, and using more detailed levels of best practice in their service offering.

5. Structure

5.1 Disclosure

The following areas of the code were identified during consultation, including the Structure and Approach survey conducted in December 2011 which saw 70% of respondents preferring a disclosure based code of practice. Additionally it was suggested via the survey and strongly voiced during consultation that additional modules be made available to organisations wishing to comply with and be recognised for a higher standard of compliance in certain areas. These modules are highlighted at the end of this section.

NOTE that the information contained in each box is a summary of the types of information expected, however the actual detail will be established during consultation in the next stage of development in early 2012.

For an organisation to be compliant with this code, they must truthfully disclose the following information to all clients, both prospective and current, before, during and after the sales process. They are required to update any disclosures and actively inform clients of these changes disclosures as soon as possible and not later than 28 days of that change being made.

Each organisation must comply with each of these requirements. An organisation may choose to subscribe to additional disclosure modules highlighting their further commitment to their standards of good practice.

The standard areas of disclosure required by this code are:

Corporate Identity

Details of the legal entity and its trading name if applicable. Trading start date, physical office location, postal address, contract phone, fax and email details. This section could also include details of major shareholders of the trading entity, CEO (or equivalents) details. This is also an opportunity for the company to declare that it complies with the code and any additional modules that they may also subscribe to.

Ownership of Data

A preformatted statement disclosing who owns the data (ie the supplier or the client) once housed on the suppliers service and details of any circumstances that the ownership of the data may change.

Security

Statements and disclosures regarding security practices used. This section will also require compliance to one of a set of minimum security standards (eg such as defined by NIST, CSA or other established/recognised standards) or other such similar standards as determined by the security focus group as a suitable standard to work with.

Data Location

A Preformatted statement disclosing in what country or jurisdiction data is stored and for what purpose, ie it is permanently housed offshore, the data is mirrored or backed up off shore etc. This statement should also include wording to highlight that offshore data may become subject to international law and any other consequences of data being offshore, and referring to a page on the Privacy Commission's site outlining any risks associated with hosting in certain countries

Data Access

Details of how data can be accessed both during the service provision and if it is available (and under what circumstances) after the contract has ceased. This will also include disclosure of any proprietary elements to the way data is stored and accessed and if and how data may be exported to a standard format used by other providers

Back up and maintenance

A preformatted statement stating the providers back up process, and regular maintenance program. This should also include how they intend to communicate with the client regarding scheduled maintainence and service disruptions

Geographic Diversity

A Statement disclosing the countries in which services are provided from and the consequence of the service being provided from that location (if any) as determined independently

SLA and Support

Details of uptime SLAs, general support hours and how to contact the suppliers support team. This should also include details of how the supplier will communicate with the client when unexpected service disruptions have occurred and the availabilty of support services (eg 9-5pm, 24 hours, etc) based on the severity of the issue.

Competency warranty

A Statement declaring that the provider is capable of providing the services as set out in their terms and conditions.

Privacy Policy

Declaration of the service providers Privacy Policy including a link to such document and details of how they comply with the NZ privacy Act etc

5.2 Additional Modules

Cloud Providers may subscribe to the following additional models should they wish to promote a higher level of compliance to their clients.

It is proposed that organisations that subscribe to these additional modules to the code are recognised in some way. This could be in a number of ways, such as a being recognised as a teir1, 2 3 or 4 Code compliant organisation based on the number of modules they subscribe to, or creating some kind of additional levels system. It is intended that the logo that these organisations would use would be recognisably different to the standard code compliance logo. The use of additional modules now allows for future proofing in moving towards a multi-tiered structure in the future.

Enhanced security

To include details of their incident reporting and breach policies including that of their third party provider (if applicable), levels of encryption used, user authentication methods used. Details of measures in place for both security of hardware /networks and data security.

Data Transportability

More detained disclosure of customer migration paths for data during the service being provided and after the service has been ceased and costs related in this service being provided.

Service Dependencies

Include names of upstream providers, and what provisions will be made if the upstream supplier goes out of business, sells or merges their business with another, or other such acts which may affect the supplier's client. Details should also be provided regarding what happens when the upstream service provider suffers a service disruption. Whether the upstream provider has access to client data, and details of compensation available from the service provider if the upstream provider is responsible for an issue.

Business Continuity

A Statement or list of declarations regarding the Service Providers Business Continuity plan

HR/Personal procedures.

Statement or check list of HR procedures surrounding pre-employment security checks of technical staff and qualifications held.

Data Formats

Disclosure of data formats used – details of proprietary data formats used (if any) and details of any portability / interoperability standards that the business/service supports.

Jurisdictions

Disclosure of Jurisdictions that are relevant to the service being supplied.

5.3 Customer Engagement

This section of the code set the standards of conduct that we expect to see cloud providers engage in and require them to confirm that they act lawfully within the Privacy Act, Fairtrading Act, and any other relevant legislations. It will also provide a mechanism for complaints handling (internally and if that fails, through the Code process).

5.4 Assessment

63% of survey participants preferred self assessment; however 52% preferred either a mix of randomised 3rd party assessments or compulsory assessment. 60% of participants agree that an organisation should sit over top of the Code to ensure it is developed monitored and grown appropriately

This section should outline how the code is assessed and who by and at what frequency.

While the final Cloud Code from this process will include a recommendation, the full details of this section are outside the scope of this part of the project.

5.5 Recognition of Compliance to this code.

Organisations that are compliant with the code of practice will be authorised to use a code of practice compliance logo on their marketing and website (which must link back to the code of practice website).

The Code will also specify specific wording that can be used in marketing collatoral, tender responses and quotes. Promotion of the Code will be restricted to specific wording to ensure consistency, clarity in terms of what this means and providing uniformity in the way the code of practice is promoted to the public.

5.6 Maintenance of this code

This section will detail how this code will be maintained, by whom and how often. It will also offer a complaints resolution procedure for dealing with claims that a provider is not complying with the Code (following unsatisfactory internal resolution).

6. Reference Material

Further information with relation to the development of this code of practice can be found in the following documents available on www.nzcloudcode.org.nz:

- Survey Summary – Structure and Approach 2011.pdf
- Cloud Code ToR Final.pdf

We also recommend the NIST definition document available here
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf