

NEW ZEALAND CLOUD COMPUTING CODE OF PRACTICE

Version 1.01 (June 2012)

*New Zealand Cloud Computing Code of Practice.
Published by the Institute of IT Professionals NZ Inc
(formerly NZCS) in May 2012. This version June 2012.*



**Institute of IT
Professionals**
NEW ZEALAND

Table of contents

1. Introduction	1
1.1 Core Principles of the Code	
1.2 Aims of the Code	
2. Defining Cloud	3
2.1 What is Cloud computing?	
3. Application	4
3.1 Who does this Code of Practice apply to?	
4. Approach	4
4.1 Cloud Code of Practice to relate to Provider's Products or Services	
4.2 Compliance with the Code of Practice	
4.3 Fees	
4.4 Withdrawal from this Code of Practice	
5. Code of Practice Disclosures	6
5.1 Disclosure	
5.2 Corporate Identity	
5.3 Ownership of Data	
5.4 Security	
5.5 Data Location	
5.6 Data Access and Use	
5.7 Back up and maintenance	
5.8 Geographic Diversity	
5.9 SLA and Support	
5.10 Data Breach Notification	
5.11 Data Transportability	
5.12 Business Continuity	
5.13 Data Formats	
5.14 Ownership of Application	
6. Customer Engagement	12
7. Assessment	13
8. Recognition of Compliance to this code	13
9. Maintenance of this code	13
Schedule 1: Fair trading compliance policy	14
Schedule 2: Cloud Security Alliance STAR Registry Information	17
Schedule 3: Security Standards List	18

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 requirements of The Code, and receiving recognition via use of a distinguished mark and entry into a register of cloud providers compliant with this Code of Practice.

The Code assists end users by allowing them to make informed decisions based on the disclosure of practices of the service provider enabling end users to be confident with the service provider’s ability to meet end users requirements.

The Code also builds trust within the Cloud Service Industry by providing a trusted format which both suppliers and customers can depend on.

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 250 individuals from both around New Zealand and off-shore.

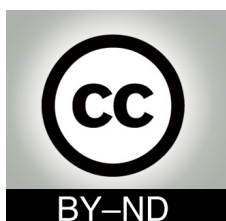


Major Contributors

Equinox Limited, Gen-i, OneNet, Webdrive, Xero, Institute of IT Professionals NZ Inc (formerly NZCS).

Other Contributors

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



This document is made available under the following license:

Creative Commons Attribution-Non Commercial 3.0 New Zealand

You are free to **share** (copy, distribute and transmit the work) under the following conditions:

- ▶ **Attribution:** You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- ▶ **No Derivative Works:** You may not alter, transform, or build upon this work.

Waiver: Note that any of these conditioned may be waived if you get permission from IITP.

Full details at <http://creativecommons.org/licenses/by-nd/3.0/nz/>

1.1 Core Principles of the Code

The following are the Core Principles for the development of the New Zealand Cloud Computing Code of Practice. These Core Principles will continue to apply during subsequent development:

- **Not Re-inventing the wheel**
Where possible, the New Zealand Cloud Computing Code of Practice leveraged 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 was researching approaches taken to addressing the core issues in overseas jurisdictions, to ensure the result was consistent with practices in other countries.
- **Research-based non-arbitrary approach**
The recommendations and resultant Code was 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/IITP and the project team was 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 worked towards a consensus view in terms of the structure and content of the Code. While consensus does not mean unanimous, the intention was to gain the wide support of a broad range of stakeholders.
- **Clear separation between governance of process and development of Code**
The steering group governed the process, ensuring the principles were adhered, to and tested the evidence based approach, however did not guide or influence the final result and code.
- **Compliance and Assessment**
It was 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 was necessary for the integrity of the code.

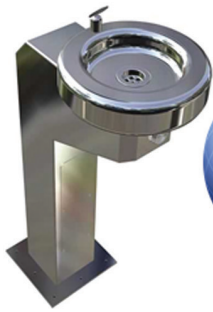
1.2 Aims of the Code

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 suppliers and customers with regards to data protection, sovereignty and privacy.
- Strengthen the integrity of Cloud Computing in New Zealand.

② Defining Cloud

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 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 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 offer remotely hosted IT services of any type, either to New Zealand or within New Zealand, that meet the definition of Cloud Computing as outlined above.

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 on a case by case basis.

The New Zealand Cloud Computing Code of Practice is a voluntary code of practice and by complying to The Code a service provider represents to the public that they comply with the Code's requirements.

The New Zealand Cloud Computing Code of Practice does not in any way place legal obligations on any of the parties participating in the Code, however non compliance with the code by a code signatory could result in liability under general law (e.g. for misleading and deceptive conduct under the Fair Trading Act 1986).

④ Approach

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

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

Providers whose offerings meet the test of compliance stated in Clause 4.2 may state that they are compliant with this Code of Practice.

The products or services to which the disclosure statements apply under this code of practice must be described in Clause 5.2 of this document

4.2 Compliance with the Code of Practice

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

- Comply with the Code's minimum security requirements at all times as described in clause 5.4.
- Ensure that the product and services as described in Section 5.2 are provided in accordance with the disclosures made in Section 5 of this code, and continually do so.
- Make and act in accordance with the Code's disclosure statements.
- Maintain a professional level of service to their clients.
- 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.
- Provide a link to their disclosure statements on their publicly available website.
- Promote the Code on their site via a link to the NZ Cloud Code of Practice website.

- NOT market any product or services specified in section 5.2 as a “Cloud” product or service unless it meets the cloud definition as above.
- NOT market any product or services specified in section 5.2 as a “Cloud” product unless it meets all base requirements of the Code
- Undertake any formal assessment or review as determined from time to time by the organisation responsible for the operation of The Code and pay any prescribed fee
- Be registered on a publicly available *Register of Cloud Providers compliant with this Code of Practice*

4.3 Fees

Organisations wishing to have their products and services recognised under this Code of Practice as being compliant must pay an annual subscription fee to be included in the registry of cloud compliant providers and use the associated marks and logos. This fee will reflect the cost of operating the Register and service and will be published on the CloudCode website. Any change to this fee, or addition of new fees will be advised on The Cloud Code website and directly to existing cloud compliant organisations in writing 90 days before such change is implemented.

4.4 Withdrawal from this Code of Practice

An organisation that wishes to withdraw from this Code of Practice must:

- Provide 60 days notice to the organisation responsible for administering the code of practice as detailed in schedule 3, in writing of their intention to withdraw
- Advise all existing clients by email that they intend to withdraw from the code of Practice at least 45 days prior to their removal from the register.
- Remove all marks and references to their adherence to this Code of Practice from all marketing material and websites prior to their removal from the register.
- No longer promote any of their products or services as being compliant with this code of practice.

5 Code of Practice Disclosures

5.1 Disclosure

For an organisation to be compliant with this Code of Practice 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 their clients in writing, and the registry, of these changed disclosures as soon as possible and not later than 28 days of that change being made.

The applying 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:

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 <http://www.....>
-as described at <http://www.....>
-as described at <http://www.....>
-as described at <http://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 beenSelf Assessed

Or

Assessed externally by(state auditing company'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**
- Meta data 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 imperative. Providers must either register in the Cloud Security Alliance STAR registry or have been formally assessed as complying with one or more of the standards listed in Schedule 3.

More information about the STAR Registry and other standards can be found in schedules 2 and 3. Cloud Service Providers who are currently undergoing the process of being added to the STAR registry will be given a pending status to their compliance to the code and are expected to have completed the process within 30 days of their application

- As at the date of application: (select the statement that applies)
- We are currently undergoing the process of acquiring the Cloud Security Alliance STAR registration, Or
We formally meet one or more of the security related standards contained in Schedule 3. Specifically(state standards held)
- The service which we provide to you is done so via a **Multi Tenanted Server / Virtual Machine / Private Virtual Machine**.

5.5 Data Location

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
 - o (if answer above is “will be available”) Access to this data will be granted via
.....(state method)
 - o There **will / will not** be additional charges for access to your data after the service has been ceased

Data access by us

- o Deletion of all customer data at the cessation of our service to you takes place
.....(state timeframe)
- o We use customer data for the following business functions
 - List item 1
 - List item 2
 - List item 3
- o We do not access customer data for any other purpose
- o We **do/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.....
.....(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 Back up 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: eg 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) distant 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, ie 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 must 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*)
 - o Our services are approximately.....km apart in distance
 - Or
 - o Our services are provided via both onshore and offshore locations
- (OPTIONAL) Our services are provided from the following locations (stating the cities and countries where services are being provided from)
- We operate offices in the following countries

5.9 SLA and Support

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 their services.

- Our standard support hours are.....(local NZ 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(eg 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.
- We classify incidents and therefore the resolution time to issues in the following way

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

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 Breach Notification

Understanding what will happen when there is a data breach is important. 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

- If we discover that your data has been lost or compromised, we will notify you as soon as practicable by(state means), unless that notification would compromise a criminal investigation into the breach.
- The notification **will / will not** be made consistent with the Voluntary Breach Notification Guidelines issued by the New Zealand Office of the Privacy Commissioner.
- Where we are able to determine that there has been significant loss or compromise of personal information, and a risk of harm to individuals, we **will also / will not** notify the Office of the Privacy Commissioner directly.
- When we are in possession of evidence of criminal activity associated with the breach we will notify appropriate law enforcement agencies

5.11 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.

5.12 Business Continuity

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

5.13 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

5.14 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 (ie your local network) by(state details of how the application can be run outside of the service provider's systems)

If the answers to the above disclosures are not consistent between the products listed in section 5.2, then this section can be duplicated referencing the products that each statement is applicable to.

⑥ Customer Engagement

As participants in the New Zealand Cloud Code of practice, we confirm that we 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 copy of which is attached as schedule 1 of this document
- 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
..(state URL of Privacy Policy.)

7 Assessment

This section will outline how compliance with the code is assessed, by whom and at what frequency.

The full details of this section will be released prior to the launch of the Register.

8 Recognition of compliance to this code

Organisations that are compliant with this 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 Cloud Code website).

The Code will also state specific wording which can be used in marketing collateral, 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 is promoted to the public.

9 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). The full details of this section are outside the scope of this part of the project and will be released prior to the launch of the Register

Schedule 1:

Fair trading compliance policy

FAIR TRADING COMPLIANCE POLICY (SAMPLE)

The following text can be used to create a compliant Fair Trading Compliance policy.

PURPOSE

1. The purpose of this policy is to ensure that:
 - all advertising and marketing used by *[insert name of business]* will comply with New Zealand's Fair Trading Act 1986; and
 - the advertising or marketing materials that we use and the associated activities we undertake will not (and could not) mislead or deceive our consumers.

SCOPE

2. This policy relates to all the things we say and do about the promotion and sale of the products and/or services we supply to consumers. This includes sales techniques and financing as well as advertising and marketing using print materials, broadcast advertising, electronic advertising, verbal messages and other forms of promotion.

WHY WE HAVE THIS POLICY

3. Consumers come from a wide range of social, cultural and educational backgrounds. Because of this, we need to be clear about the things we say and in doing so we reduce the risk of consumers misinterpreting our intentions or of us misleading them and therefore potentially breaching the Fair Trading Act.
4. The benefits for *[insert name of business]* having in place a Fair Trading Act policy and compliance programme include:
 - having better informed staff and improved customer service;
 - having better customer relations;
 - enhancing our business culture; and
 - maintaining and enhancing our good reputation.

RULES AND RESPONSIBILITIES

5. All advertising and related activities will be truthful and only contain statements and visual representations which ensure an overall impression that:
 - **does not** and is not likely to mislead or deceive consumers;
 - **does not** make false and misleading representations; and
 - **does not** abuse the trust of the consumer or exploit their lack of experience or knowledge.
6. All staff with trading/sales responsibilities must be informed of this policy and know how it applies to the work they do.

Managers are responsible for ensuring that their staff with trading/sales responsibilities are aware of all current promotions and advertising (representations) being made about the products and/or services that they supply.

All staff are responsible for immediately notifying suspected breaches of this policy to *[insert management / the person responsible for the promotion / advertising]*.

All staff with trading responsibilities will receive regular Fair Trading Act compliance training. Records of training must be maintained.

7. Initial Fair Trading Act induction training will cover:
 - awareness of this policy;
 - the responsibilities of staff and management relating to Fair Trading Act compliance; activities;
 - what is a false or misleading representation; and
 - what to do if a breach of this policy occurs.
8. *[insert name of position or person]* will be responsible for the education and compliance activities associated with this policy and the Fair Trading Act.
9. All marketing decisions and strategies will be reviewed by management to ensure they meet the requirements of this policy.
10. Product managers (or others with product management responsibilities) are responsible for ensuring that all advertising is fit for purpose and checked for compliance with this policy **before** it is cleared for use.
11. An in-house system for checking and approving all publicity material against the requirements of this policy and the Fair Trading Act will be used by relevant staff, managers, contractors and advertising agencies (refer to Check Sheet 1: Fair Trading Act advertising / promotion compliance).
12. The person who checks the material should have reasonable product knowledge about the products and /or services being promoted. The person who then approves the material must have the authority to approve advertising representations in *[insert name of business]*.
13. The Fair Trading Act complaints register will be used by *[insert name of business]*.
14. All Fair Trading Act complaints made by consumers and competitors will be:
 - recorded in a complaints register;
 - managed promptly to ensure any potential breaches are rectified immediately and suitable action(s) put in place to reduce the likelihood of reoccurrence; and
 - reported periodically to *[insert senior management / the Board / other]*.
15. Any mistakes in published advertising materials will be remedied immediately, including destroying or carefully altering the advertising materials and alerting consumers to the error. As appropriate, managers should be assigned to handle any dissatisfied consumers.
16. Out of date advertising materials will longer be displayed or used in promotions.

BASICS ABOUT THE FAIR TRADING ACT

17. The following information covers the basics about the Fair Trading Act. The Act:
 - prohibits people in trade from engaging in misleading or deceptive conduct generally;
 - prohibits certain types of false or misleading representations about goods or services (e.g. false claims about skills, qualifications, success, test and survey results);
 - prohibits certain types of false or misleading representations or conduct in relation to land;
 - prohibits certain unfair trading practices (e.g. bait advertising, offering gifts as part of a promotion with no intention of supplying them or misrepresenting the nature of the gift, using packaging that misrepresents the products inside);
 - provides for consumer information and product safety standards regulations and unsafe goods notices; and
 - prohibits misleading conduct in relation to employment offers.
18. The Ministry of Consumer Affairs is responsible for administering the Fair Trading Act, including reporting to Government on the need for changes to the current law and other policy matters. The Minister also has the power to order compulsory recall of goods which fail to meet a product safety standard or which may cause injury.
19. The Commerce Commission is responsible for enforcing the Fair Trading Act. In taking action against a business that may have breached the Act, the Commerce Commission's focus is not on whether *[insert name of business]* ever intended to deceive or mislead consumers, but whether the things we have said and done are liable, or likely, to deceive or mislead consumers.

DEFINITIONS AND EXAMPLES

Advertising	Any form of communication made to the public or a section of the public for the purpose of promoting the supply of products or services or the sale of property. Examples include: <ul style="list-style-type: none"> • broadcast advertising. This can include television and radio advertising and infomercials; • electronic advertising. This can include website, text messages and email; • print materials. This can include product labelling, guarantees, pledges, mailers, flyers, newspapers, brochures, magazine and journal advertisements, billboards, point-of-sale and other display material; and • verbal messages. This can include sales pitches, promises and general product and service information provided verbally in person or by phone.
Complaints handling system	A customer feedback system for collecting and recording complaints about our Fair Trading Act compliance activities. An effective complaints handling system enables us to properly manage each complaint and learn and improve on what we do.
Deceive	To cause to believe what is false, to mislead as to a matter of fact, to lead into error; to delude, take in.
Mislead	To lead astray in action or conduct, to lead into error, to cause to err.
Representation	A representation is any factual statement made about a product or service, either orally or in writing. A representation may also be an impression given by pictures, advertisements, promotional material or a sales pitch, by general conduct, including by keeping silent when critical information should be given. Representations can also be made in specifications and product descriptions, warranties and contracts.
Supply	For products, supply can include supply by gift, sale, exchanges, lease, hire or hire purchase. For services, supply can include the providing or giving of a service.
Trade	Any trade, business, industry, profession, occupation, activity of commerce or undertaking relating to the supply or getting of products or services or land. Few undertakings, except one-off private transactions, escape the jurisdiction of the Fair Trading Act.

INFORMATION SOURCES

20. More information about the Fair Trading Act and achieving compliance with the Act can be obtained from the following sources:

- The Fair Trading Act 1986 www.legislation.govt.nz
- Ministry of Consumer Affairs www.consumeraffairs.govt.nz
- Commerce Commission www.comcom.govt.nz
- The Advertising Standards Authority www.asa.co.nz

This policy is authorised by:

.....

Name and position *Date*

Disclaimer

These compliance resources are guides only and reflect the Commerce Commission's view. Use of these compliance resources does not in itself guarantee compliance with the Act. However, an effective compliance programme, properly implemented, should mitigate the risk of contravening the Act.

Only the courts can make an authoritative ruling on breaches of the Fair Trading Act. These compliance resources are not intended to be definitive and should not be used instead of legal advice.

Schedule 2:

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.

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 here: <https://cloudsecurityalliance.org/star/>

Schedule 3:

Security Standards List

The list of additional security Standards will be released prior to the launch of the CloudCode Registry.