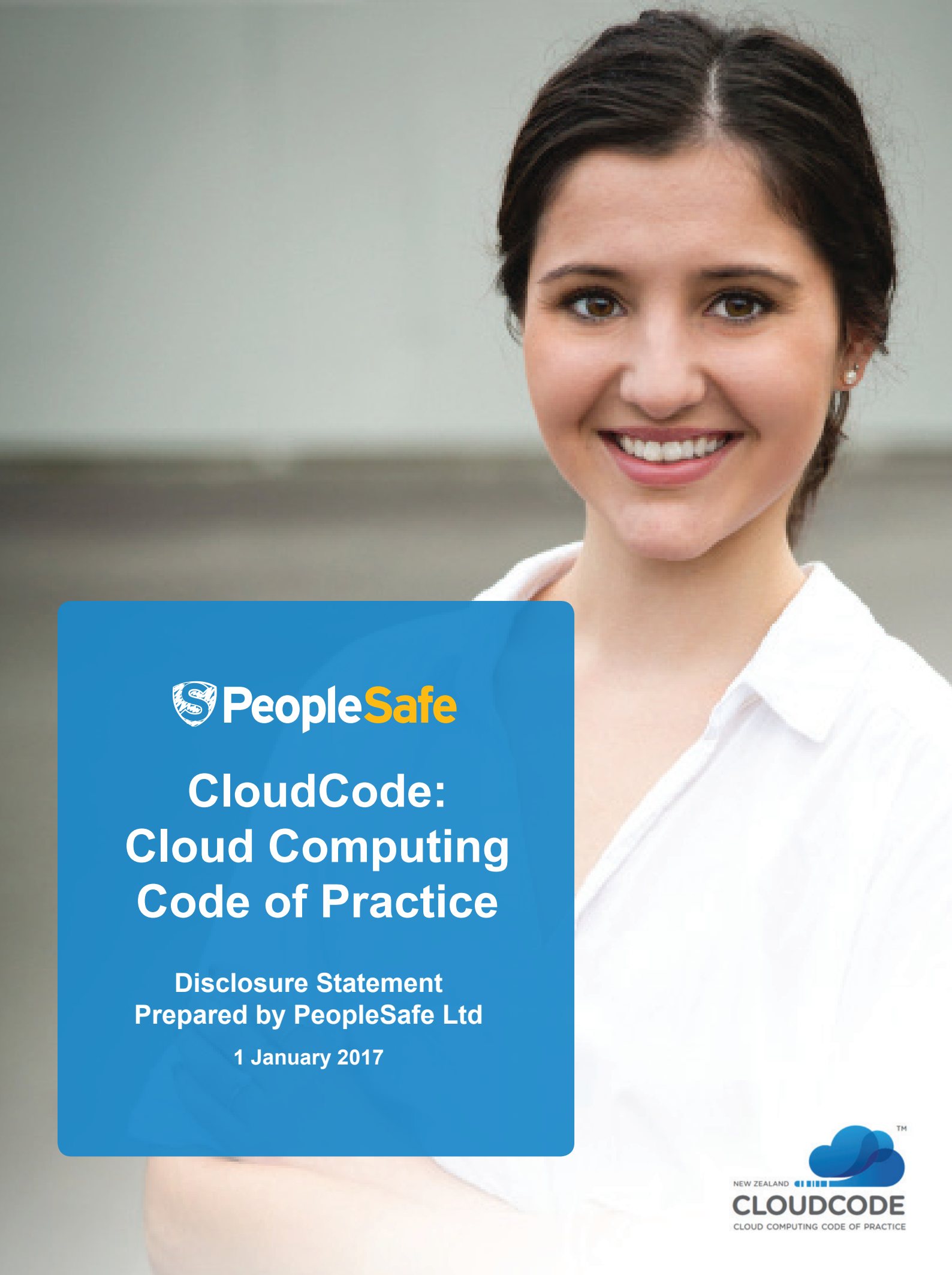

PeopleSafe

CloudCode: Cloud Computing Code of Practice

Disclosure Statement
Prepared by PeopleSafe Ltd

1 January 2017

NEW ZEALAND CLOUDCODE™
CLOUD COMPUTING CODE OF PRACTICE

Introduction

For an organisation to be a CloudCode Signatory they must wholly disclose the following information to all clients, both prospective and current, before, during and after the sales process. They must update their Disclosure Document and inform the Register of CloudCode Signatories of these changed disclosures as soon as possible and not later than 28 days after the change is made. Where the change has a material effect on the Cloud product or service being provided, they must notify all clients of these changes.

1 Corporate Identity

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

Company name:	**PeopleSafe Ltd**
Company Registration Number:	**3265828**
Trading name:	**PeopleSafe**
Physical address:	**227 Broadway Avenue, Palmerston North 4414**
Postal address:	**P.O. Box 2004, Palmerston North 4440**
Company website:	**http://www.peoplesafe.co.nz**
Contact phone number:	**Freephone: 0800 111 558** **International: +64 6 350 0006**
Contact email address:	**help@peoplesafe.co.nz**

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

Contact:
Operations Manager
PeopleSafe Ltd
P.O. Box 2004,
Palmerston North 4440

Email:
service@peoplesafe.co.nz

Contact person responsible for these disclosure statements can be contacted via:
disclosure@peoplesafe.co.nz

- **The disclosures herein apply to the following products and services supplied by us:**
  - **PeopleSafe online safety software**, as described at **www.peoplesafe.co.nz**
- For the purpose of Legal Jurisdiction, the contracted supplier who provides the service to you is a **Limited Liability Company** registered in **New Zealand.**
- The governing law of our contract with you is **New Zealand law.**
- The disclosure statements that follow have been **Self Assessed** by **PeopleSafe Ltd Management and IT Team.**

2 Ownership of Information

- We **do not** claim ownership of any data or information uploaded to our service.
- Your data and information may traverse or be stored on our upstream provider's networks or systems. In these instances that provider considers the data and information that you use or transmit via our service is owned by **the respective clients of PeopleSafe Ltd.**
- Metadata and other statistical information, such as anonymised data generated as a result of the use of our service, is **owned by PeopleSafe Ltd as the service provider** and may be used for the purposes of **producing industry summary statistics, summary usage benchmarking, system performance analysis, and service delivery improvements.**

3 Security

As at the date of application:

- We **are not** listed on the CSA STAR Registry.
- We are currently undergoing the process of acquiring certification against the following security related standard(s): **CSA STAR Self Assessment (http://www.cloudsecurityalliance.org/star/self-assessment)**
- We have the following physical security in place at the data centres hosting your data: **High-grade dedicated facility with 24x7x365 onsite staff; 24x7x365 monitoring including alarms and CCTV surveillance with recording; entry control systems, with supervised access only.**
- We have the following digital security in place on the systems hosting your data: **Multiple firewall layers, with 24/7/365 firewall monitoring and management; Intrusion Prevention System; External security audits; Complex password policies; Restricted administrator-level access; SSL encrypted communications.**

4 Data Location

- ☑ Our primary systems that host your data are located in **Auckland, New Zealand.**
- ☑ Our Backup/Disaster recovery systems that hold your data are located in **Christchurch, New Zealand and Palmerston North, New Zealand.**

Additional information about data location:

Our primary datacentre, primary onsite backup provider, and secondary offsite backup provider, is ICONZ-Webvisions, Auckland. Our secondary datacentre is located in Christchurch. Our secondary offsite backups are located in Palmerston North.

5 Data Access and Use

Data access by you:

- Your data may be accessed during the contract period as described in our contract with you.
- Your data can be downloaded from our service during the service provision period via the following formats: **HTML, PDF, and CSV reports; Original file formats of documents uploaded.**
- At the cessation of our service to you, your data **will not** be available to access.

Data access by us:

- Deletion of all customer data at the cessation of our service to you takes place **90 days** after the cessation of our service to you.

  We use customer data for the following business functions

  - **Service communications and billing.**
  - **Usage metadata for industry statistics and activity benchmarking.**
  - **We do not use identifiable company data for any other business function.**
- We **do not** access customer data for any other purpose, **unless granted "Auditor" or "Advisor" access by the customer, for the sole benefit of the customer.**
- We **do not** use customer data in order to generate revenue other than through provision of the service.

Data access by others:

- If we are approached by law enforcement agencies it is our policy to **comply with legal requests to provide access to data to the extent required under New Zealand law.**
- We **do not** provide access to customer data to third parties other than law enforcement agencies as set out above.

6 Backup and Maintenance

Understanding the backup procedures of your service provider and their maintenance policies allows the customer to make decisions on what further steps they may need to ensure their data is backed up sufficiently.

Backups are performed hourly (24x7), and daily.

Backups include:

- ☑ System data
- ☑ Client data
- ☑ Statistical data
- ☑ Operating system data

- Backup data is stored **Onsite; Offsite Auckland; and Offsite Palmerston North**
- Where backup data is stored offsite, the remote offsite location is **18Km and 500 Km** from the location of the data being backed up.
- We test the restoration of backup data every **3 months, and periodically between;** and the test is **conducted as a full system and data restore; and periodic data restore only. Restoration is validated via our data integrity and system test routines.**
- Access to backup data or archive data **is not** available.
- Adhoc requests for restoration of customer data are **not** provided for.
- We **do not** allow client audits of backup data.
- Backup data is retained for **12 months.**
- We **do** undertake a regular maintenance programme to ensure the reliability and stability of our cloud resources.

7 Geographic Diversity

- Our service is provided via multiple locations.
- Our services are provided from the following locations: **Auckland, New Zealand, Palmerston North, New Zealand, and Christchurch, New Zealand.**
- Our services are approximately **500 Km** apart in distance
- We operate offices in the following countries: **New Zealand**

8 SLA and Support

This section sets out the standard support mechanisms and service level agreements that apply to services.

- ☑ Our standard support hours are **Monday – Friday, 9:00 AM – 5:00 PM (NZT).**
- ☑ In the event of an unscheduled outage or incident, we will communicate details of the issues and expected resolution times **via our status page: http://status.peoplesafe.co.nz; and Twitter: @PeopleSafe_HQ**
- ☑ When communicating an issue to us we prefer you to do so via **a support request from our support portal: http://help.peoplesafe.co.nz, or email to help@peoplesafe.co.nz**
- ☑ Our standard response time to any support issue is raised **within 1 business day.**
- ☑ In the event of a major incident, we will update our notifications **every hour.**
- ☑ When communicating with you we will use **the Main Contact Person email and/or phone specified at Signup, or as updated by the customer in their Organisation Details.**
- ☑ We **do** make incident reports available to our clients after a major incident.
- ☑ We **will** shut down or isolate any service offering that is impacting, or will impact, service level agreements.
- ☑ We **may** require service offering specific tools to enable safe service offering shutdown or isolation if needed.
- ☑ We operate an **active/active** based service.

Our Service Level target is 99.9% application availability; supported by 99.98% infrastructure target availability. We have 24x7x365 monitoring of system availability; system load; and application performance. We have 24x7x365 onsite support at the infrastructure level, and 16x5 support at the application level.

9 Data Transportability

- We **may** allow the use of an API to access data during service provisioning and consumption.
- Data **will not** be available to download after we cease supplying service to you.
- There **will** be additional charges associated with accessing data after your service has ceased. **This would require you to make arrangements with PeopleSafe for accessing such Data prior to the deletion of that Data which, as referred to above, shall take place 90 days after cessation of our Service to You.**

10 Business Continuity

Our primary application environment is based on a cluster of physical host servers spread between two levels of our provider's Auckland datacentre. This cluster is connected to a redundant pair of SAN's. The cluster is protected from power failure by an n+1 redundant UPS system backed by two onsite generators. Both levels of the datacentre feature redundant process cooler systems.

The primary datacentre's core network is fully redundant, including links from the host cluster to the core, from the core to all connections. The datacenter peers with all major NZ networks with international connectivity served over three redundant international links with two separate carriers.

The primary datacenter has 24x7x365 onsite engineers with a platform availability target of 99.98%.

Our Disaster Recovery plans, as a subset of our Business Continuity plans include multiple levels of onsite (Auckland) and offsite backups (Auckland and Palmerston North); a 'warm-spare' standby hosting environment within our primary datacenter (Auckland), and a standby hosting environment located in a geographically and functionally separate datacenter located in Christchurch.

Our development and support teams are located between two offices in Palmerston North. In this we have independence from possible events in Auckland and availability of full backups (system snapshots, and hourly data) from Palmerston North, for possible worst-case deployment to Christchurch.

Our Palmerston North offices have independent communication networks and power supplies, and key personnel fully equipped to work remotely.

Our continuity plans are regularly reviewed and tested.

11 Data Formats

- All client data **can** be exported at any stage of the service delivery. **Individual records, and category-specific reports can be extracted in HTML, PDF, and CSV formats at any time. Stored documents can be retrieved in the same formats as originally uploaded.**

- Our API requires data to be transmitted in the following formats: **N/A. Under development at time of Disclosure.**

12 Ownership of Application

- The source code for the applications that you use on our service is **not** available to license on your systems outside of our service provision.
- It will **not** be possible to use your data downloaded from our systems in its native form outside of our service.

13 Customer Engagement

- We **do not** allow the auditing of our services by customers
- We **do** have an acceptable use policy that is applicable to the services stated in section 5.2. This policy can be found at **http://www.peoplesafe.co.nz/terms-of-use**
- We **do** operate a Privacy Policy. This policy can be found at **http://www.peoplesafe.co.nz/privacy**

14 Data Breaches

- If we discover that your data has been lost or compromised, we will **always** notify you as soon as practicable by **email** to the **Main Contact Person specified at Signup, or as updated by the customer in their Organisation Details,** unless that notification would compromise a criminal investigation into the breach.
- When we are in possession of evidence of criminal activity associated with the breach (such as evidence of hacker activity) we will **always** notify appropriate law enforcement agencies.

15 Law Enforcement

When requested by appropriate law enforcement agencies to supply customer related information without a warrant or legal mechanism to compel disclosure:

- It is our usual policy **not to** comply with such requests.

16 Region specific Disclosures

Countries to which we are becoming a signatory to the CloudCode:

- **New Zealand only.**

Schedule 1
New Zealand Specific Content

S1.1 Data Breach Notification

The Office of the Privacy Commissioner has published voluntary breach notification guidelines, which can be found at www.privacy.org.nz/privacy-breach-guidelines-2

- ☑ The Data Breach Notification we will make in Section 5.15 **will** be made consistent with the Voluntary Breach Notification Guidelines issued by the Office of the Privacy Commissioner in New Zealand.

- ☑ Where we are able to determine that there has been significant loss or compromise of information and a risk of harm to individuals we **will also** notify the Office of the Privacy Commissioner directly.

S1.2 New Zealand Legislation

- ☑ We affirm that we always comply with the Privacy Act, Fair Trading Act, Commerce Act, Copyright (Infringing File Sharing) Amendment Act 2011 and other relevant legislation.

- ☑ We **do** have a current Fair Trading Act Compliance policy, a copy of which is **available from http://www.peoplesafe.co.nz/fairtradingact**

PeopleSafe

CloudCode: Cloud Computing Code of Practice

Disclosure Statement
Prepared by PeopleSafe Ltd

1 January 2017

NEW ZEALAND CLOUDCODE™
CLOUD COMPUTING CODE OF PRACTICE