# Tasmanian Cloud Policy

Version 1.0, October 2015

Department of Premier and Cabinet
Office of eGovernment

Tasmania
Explore the possibilities

# CONTENTS

# 1 Introduction and context

## 1.1 Scope

This policy applies to agencies as defined in the *Financial Management and Audit Act 1990* and relates to information and communications technology (ICT) server equipment, storage systems, and data centre facilities.

This policy does not change, or limit, the organisations that may purchase Tasmanian Cloud services via the Networking Tasmania agreements.

## 1.2 Government policy

The Tasmanian Government's "Growing our Information and Communications Technology (ICT) policy" outlines a data centre action strategy for Tasmania, which includes:

> *To play our part, we will set a goal of moving whole-of-government data to the Tasmanian Cloud (secure, on-island data centres) – setting an example for other major organisations such as the University of Tasmania, local government and Tasmanian businesses.*
>
> *By establishing a four-year goal of moving to on-island data sovereignty arrangements (where all public sector data is stored on data centres within Tasmania) we will be protecting security of data, employing Tasmanians and reducing the cost of data traffic on the Bass Strait links.*

## 1.3 Networking Tasmania III

Networking Tasmanian (NT) III is the third iteration of the Tasmanian Government's outsourced managed data network arrangements. The NT III agreements are being phased in, commencing in 2015, to replace the NT II agreements.

The Tasmanian Cloud will be procured via the NT III agreements due to the strong alignment of the contract structure and that the current NT II agreements include services consistent with the Tasmanian Cloud.

The NT III agreement model:

- Allows other organisations, such as the Public Trustee, Parliament, statutory authorities, non-government schools and hospitals, local government and the University of Tasmania, to purchase services via the agreements.
- Does not require exclusive use of equipment and services for NT customers, except where sharing of equipment or services is required to meet specific service level requirements.

At the 14 November 2014 launch of the Tasmania Cloud – Networking Tasmania pre-tender consultation, the Minister for Information Technology and Innovation, the Hon Michael Ferguson MP, stated:

> *"The new Networking Tasmania agreements will be a key element in the delivery of this commitment, because these are the services which will create and support the Tasmanian Cloud.*
>
> *The Tasmanian Cloud is intended as an on-island cloud service, using services provided by multiple suppliers, which will securely support key public sector data and ICT services.*
>
> *Note the use of public cloud service by Government agencies has not been ruled out as an option for some activities.*
>
> *A new Tasmanian Government ICT Strategy is being developed through the Government's ICT Policy Board and is expected to be released in 2015. This is expected to clarify the scope and implementation of the Tasmanian Cloud policy, as it affects IT within government."*

## 1.4 Support of NT III objectives

The broader NT III project objectives include:

> All government staff to have access to all the information and services that they need to perform their role regardless of their physical location and organisation context within government, including the ability for agency staff to roam.

As part of the planning for NT III, Ernst & Young was engaged to review the proposed NT III service model and assess the feasibility of the model and identify key gaps and challenges. The findings included a recommendation to:

> *Architect, design and implement a dedicated Application Services zone for hosting application services intended to be shared across agencies/departments. This solution should accommodate cloud based solutions and application virtualisation, as well as hosted solutions.*[1]

The proposed model for the Tasmanian Cloud supports the achievement of this objective, and hence supports the broader NT III objective.

[1] Ernst & Young, *NT III Business Model Review DPAC NT III Network Transformation Consulting Services Work Package 1*, page 51, 12 May 2014

# 2 Policy

## 2.1 Statement

The Tasmanian Cloud is an on-island cloud service, using services provided by multiple suppliers and procured using the Networking Tasmania agreements, which securely supports key public sector data and ICT services.

The objective of the Tasmanian Cloud initiative is that agencies <u>must</u> locate, where this is feasible and meets agency business requirements, most of their information and services in the on-island Tasmanian Cloud.

The Tasmanian Cloud is to be achieved through whole of government Tasmanian Cloud agreements for data centre services (DCaaS) and infrastructure as a service (IaaS)[2], and related services, provided under NT which agencies <u>must</u> utilise.

Agencies utilising software as a service (SaaS) and platform as a service (PaaS) <u>should</u> ensure that such services are hosted in the Tasmanian Cloud, where feasible and meets agency business requirements.

## 2.2 Expectation and transition

By the end of 2018, all agencies:

- Will have located most of their information and services in the on-island Tasmanian Cloud through the
  - Procurement of Tasmanian Cloud DCaaS and IaaS through Networking Tasmania agreements
  - Utilisation of SaaS and PaaS that are hosted in the Tasmanian Cloud
- Will have closed their existing data centres and be progressively moving away from owning ICT server and storage equipment, and will procure any residual data centre service requirements from the Tasmanian Cloud
- May have some residual small local ICT servers (see Section 3.3)
- May have a need to locate some of the information and services outside of the Tasmanian Cloud, in order to meet agency business requirements (see Section 3.4)

[2] See Section Appendix 3 – Definitions

# 3 Guidance and practical considerations

## 3.1 Tasmanian Cloud

The Tasmanian Cloud is an on-island cloud service, using services provided by multiple suppliers through whole of government contracts, which will securely support key public sector data and ICT services.

Tasmanian Cloud service providers, except where necessary to meet specific security or other requirements of a specific service or application, are not required to provide dedicated infrastructure and associated equipment to their Tasmanian Government customers.

The Tasmanian Cloud will be procured through the Networking Tasmania (NT) arrangements and will include DCaaS and IaaS offerings, and potentially, where feasible and compatible with the NT service model, other service offerings.

## 3.2 Transition arrangements for existing ICT servers and storage

The transition period is up to the end of 2018.

In the transition period leading up to the decommissioning of agency owned and operated ICT server and storage equipment, agencies may make minor upgrades to their existing infrastructure, but <u>should</u> not purchase any new infrastructure, except in accordance with this policy.

## 3.3 Small local ICT servers

Agencies <u>may</u> install small local ICT services, such as small ICT servers and storage infrastructure, provided that the local ICT services:

1. only support users located in the same site as the local ICT server;
2. do not require additional cooling or power requirements compared to the rest of the site; and
3. are classified as low risk, and only support low risk services.

## 3.4 Information and services outside of the Tasmanian Cloud

In order to meet agency business requirements, agencies may be required to locate some information or services outside of the Tasmanian Cloud.

Typically, this will involve the utilisation by agencies of SaaS and PaaS that are not hosted in the Tasmanian Cloud.

Agencies <u>should</u> develop a business case (that considers and balances the costs, benefits and risks) if information or services are to be located outside of the Tasmanian Cloud.

As part of the business case development, agencies should undertake a cloud risk assessment (see Appendix 1 – Cloud risk assessment).

# Appendices

## Appendix 1 – Cloud risk assessment

### Risk assessment

The business owner, not agency ICT staff, should be responsible for the risk assessment. Agency ICT staff should provide input into the risk assessment. Appendix 2 – Business risk approach to ICT system risk assessment provides guidance on assessing the risk.

Agencies are required to undertake a comprehensive risk assessment in relation to the storage and maintenance of public sector information and records. This is more critical when that information and records are managed by a non-Tasmanian Cloud service provider. It is recognised that there will be some types of government information that may be unsuitable for non-Tasmanian Cloud based services.

A full understanding of the risks, as well as opportunities, associated with non-Tasmanian Cloud based solutions both from an end user and delivery capability perspective will be critical. This requires the implementation of a risk management approach to ICT delivery. Agencies' evaluation of non-Tasmanian Cloud computing options must appropriately address all identified risks and must take account of:

- Agency Business and ICT Risk Management policies
- Tasmanian Government Information Security Policy
- TAHO Managing Information Risk - State Records Guideline No 25
- AS/NZS ISO 31000 Risk management Principles and guidelines

Non-Tasmanian Cloud services are not a new technology, but rather a different ICT service delivery model. However with non-Tasmanian Cloud services there is an increased focus on the following areas of risk:

- Integrity – can the solution or service provider ensure that the services or information cannot be altered intentionally without permission?
- Information Sovereignty and Location - is the information or service hosted outside of Australia? It is likely that information hosted in public cloud services will be subject to foreign laws rather than Australian law.
- Availability – can the solution or service provider ensure that they can provide high availability?
- Privacy and Confidentiality - does the solution meet the agency privacy and confidentially risk requirements? It is likely that security and access to information may not be at a level expected within Australia, especially when considering the network path to access the service.
- Legal – are there any contractual or legal requirements that impact on the use of a non-Tasmanian Cloud?
- Business Continuity:

- internal - can the agency operate and recover from outages or disaster situation within agreed and appropriate timeframes?
- external – can the solution recover from outages or disaster situation within agreed and appropriate timeframes?

- Exit Strategies – can the agency recover if the service provider fails? Or, after the contract for the services ends are there any issues in recovering the data and transferring the service to an alternative supplier.

An example of typical risks that must be considered in a risk assessment can be found in the section below.

## Typical Risks

Depending upon the service type, business need and delivery model adopted, the following risk categories should be considered in a risk assessment for a new ICT service:

- Security:
  - internal – does the agency have the relevant security controls identified?
  - external - does the solution or service provider have sufficient security controls in place?
- Integrity – can the solution or service provider ensure that the services or information cannot be altered intentionally without permission?
- Availability – can the solution or service provider ensure that they can provide high availability?
- Privacy and Confidentiality :
  - internal - has the agency privacy and confidentially risk requirements been identified?
  - external - does the solution meet the agency privacy and confidentially risk requirements?
- Quality – does the solution meet the business and stakeholder needs?
- Financial – does the solution provide value for money, including entry and exit costs?
- Organisational – does the solution work within the agency's culture?
- Integration – can the solution meet objectives without business or technical integration difficulties?
- Compliance – does the solution comply with agency's legal, regulatory and policy obligations?
- Legal – is the solution and or service provider subject to Australian law?
- Business Continuity:
  - internal - can the agency operate and recover from outages or disaster situation within agreed and appropriate timeframes?

  - external – can the solution, or access to the solution, recover from outages or disaster situation within agreed and appropriate timeframes?
- Exit Strategies – can the agency recover if the service provider fails? Or the after the contract for the services end how quickly the agency's information can be recovered or if at all.
- Performance – can the service provider demonstrate appropriate performance requirements
- Information Sovereignty and Location - is the information or service hosted outside of Australia? It is likely that information hosted in public cloud services will be subject to foreign laws rather than Australian law.
- Licensing – do the existing software licensing models translate to the solution?
- Funding – does the agency have sufficient recurrent funding to run and maintain the service? As a service based models usually require little or no capital investment and usually the service charged on a recurrent funding model.
- Total Cost of Ownership – has the agency fully costed the service for the life of the service, including estimated entry and exit costs?

## Appendix 2 – Business risk approach to ICT system risk assessment

It is the responsibility of the Business Owner to determine and sign off on the risk level of ICT services. The table below guides the risk assessment.

Most government systems are likely to have a risk level of medium or low. Some systems may have a high risk level for only one element.

For example, a system providing a critical public facing service may have a general risk level of medium, qualified with high (availability).

| Risk Level | Assessment Result | Assess the risk of the application or service against each of the 3 columns below | | |
|---|---|---|---|---|
| | | *Confidentiality* | *Integrity* | *Availability** |
| High | Any High identified in one of the 3 assessment columns results in a High for that element. | Information that if its confidentiality was compromised could cause damage to the State Government Commercial entities or members of the public | Extremely damaging.<br>Unauthorized alteration would seriously and adversely impact, the Tasmanian Government, its business partners, and/or its customers. | Critical.<br>Information or service that if unavailable for even a few hours would seriously and adversely impact the Tasmanian Government, its business partners, and/or its customers |
| Medium | Any Medium identified in one the 3 assessment columns and no Highs results in a Medium overall | Information that if its confidentiality was compromised could cause limited damage to the State Government Commercial entities or members of the public | Moderately damaging.<br>Alteration could adversely impact, the Tasmanian Government, its business partners, its employees, and/or its customers | Important.<br>Information or service that if unavailable for several hours to a few days could adversely impact the Tasmanian Government, its business partners, its employees, and/or its customers. |
| Low | All Lows identified in the 3 assessment columns results in a Low overall | Information that if its confidentiality was compromised may undermine public confidence in government operations.<br>or<br>Information that has been authorised for public access and circulation | Not damaging.<br>The unauthorized alteration of this information is not expected to seriously or adversely impact the agency, its employees, the Tasmanian Government, its business partners, and/or its customers. | Non-critical.<br>Information or service that if unavailable for several days would not seriously or adversely impact the agency, its employees, the Tasmanian Government, its business partners, and/or its customers |

* ICT system or service availability requirements must should may be determined as part of the business continuity planning process.

## Appendix 3 – Definitions

DCaaS	Data Centre as a Service – Provision, as a service, managed computing racks and associated infrastructure. The purchaser installs their ICT equipment into the managed racks.

IaaS	Infrastructure as a Service – Provision, as a service, of physical or virtual computing resources, computer storage (ie disk space), and related services. The purchaser installs their operating system images and application software on the cloud infrastructure.

ICT	Information and communications technology – computer and communications technology, including telephony, computer hardware and software, and related services.

NT	Networking Tasmania – The Tasmanian Government wide area network agreements which provide network as a service, and related services, to eligible customers.

PaaS	Platform as a Service – Provision, as a service, a computing platform, such as a development tools, database or web server, which allows the purchasers to deploy their software services.

SaaS	Software as a Service – Provision, as a service, access to application software and databases. The provider is responsible for sourcing and managing the underlying infrastructure.