Cloud Computing Policy and Guidelines

July 2011
Version 1.0
## Document Control

### Document details

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Cloud computing Policy and Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact details</td>
<td>Information Communication Technology (ICT) Policy and Strategy Division, Department of Corporate and Information Services (DCIS) Northern Territory Government (NTG).</td>
</tr>
<tr>
<td>File name</td>
<td>lt_ict_cloud_computing_policy_guidelines</td>
</tr>
<tr>
<td>Version</td>
<td>Version 1.1</td>
</tr>
<tr>
<td>Date issued</td>
<td>January 2013</td>
</tr>
<tr>
<td>Approved by</td>
<td>NTG CIO Forum: 27 October 2011</td>
</tr>
</tbody>
</table>

### Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Change details</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.2</td>
<td>6 Jul 2011</td>
<td>Brian Chilcott</td>
<td>Initial draft</td>
</tr>
<tr>
<td>1.0</td>
<td>26 Oct 2011</td>
<td>Brian Chilcott</td>
<td>Endorsed by NTG CIO Forum</td>
</tr>
<tr>
<td>1.1</td>
<td>14 Jan 2013</td>
<td>K. McCarthy</td>
<td>Updated government names.</td>
</tr>
</tbody>
</table>
# Table of Contents

1 Policy Statement .............................................................................................................4  
   1.1 Overview ..................................................................................................................4  
   1.2 Purpose ....................................................................................................................4  
   1.3 Scope .......................................................................................................................4  
   1.4 Responsibility ..........................................................................................................4  

2 Definition .........................................................................................................................5  
   2.1 Types of Cloud Computing .......................................................................................6  
   2.2 Cloud Service Capability .........................................................................................6  
   2.3 Maturity of Cloud Computing ..................................................................................7  

3 Drivers, risks and benefits ...............................................................................................8  
   3.1 Drivers ......................................................................................................................8  
   3.2 Potential risks of cloud computing .........................................................................9  
   3.4 Potential benefits of cloud computing ..................................................................12  

5 Guidelines ......................................................................................................................14  
   5.1 Tactical application .................................................................................................14  
   5.2 Three initial areas to test .......................................................................................14  
   5.2.1 Value for money test .........................................................................................14  
   5.2.2 Security test .......................................................................................................15  
   5.2.3 Privacy test .........................................................................................................15  
   5.3 Checklists ................................................................................................................17  

Appendix 1 – Information Act and Records Management Standards .........................18  
Appendix 2 – Information Privacy Principles .................................................................19  
Schedule 2 Information Privacy Principles ....................................................................19  

6 References ......................................................................................................................27  

Department of  
Corporate and Information Services
1 Policy Statement
The Northern Territory Government (NTG) and its agencies may choose cloud based services if they demonstrate value for money and adequate security and privacy.

1.1 Overview
Consumer demand is currently driving vendor activities in three broad infrastructure areas. These are mobile devices, wireless technology and cloud computing. Electronic content eco-systems are driving this demand and include on-line book, music and apps stores.

The maturity of consumer based cloud computing is now at a stage where governments can seriously consider the use of this technology to deliver some government services at lower costs than traditional methods.

1.2 Purpose
This policy provides guidance to NTG agencies when considering public cloud computing solutions and that information in these systems are hosted in accordance with the Information Act.

1.3 Scope
This policy applies to all decisions where services, applications, data or platforms are hosted outside the NTG’s private cloud or hosting environment.

1.4 Responsibility
The Information Communication Technology (ICT) Policy and Strategy Division of the Department of Corporate and Information Services (DCIS) is responsible for developing and maintaining ICT policies and guidelines for use across the NTG.

All NTG Chief Executives (CE) are responsible for ensuring all aspects of this policy are applied within their agency.

All NTG employees involved in procuring public cloud based services, applications or platform hosting services for the NTG must adhere to this policy.
2 Definition

The NTG has adopted the Australian Government’s definition for cloud computing. The Australian Government’s definition is in turn based on the US Government’s National Institute of Standards and Technology (NIST) definition for cloud computing.

Cloud computing is an ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model promotes availability and is composed of five essential characteristics:

- **On demand self-service** – a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

- **Broad network access** – capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs).

- **Resource pooling** – the provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or data centre).

Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- **Rapid elasticity** – capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale and be rapidly released to quickly scale in.

To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- **Measured Service** – cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts).

Resource usage can be monitored, controlled and reported; providing transparency for both the provider and consumer of the utilised service.

Cloud computing is the result of several technology advances including:

- reliable, high-speed networks, such as the National Broadband Network (NBN);
- very large, global-class infrastructures deployed by vendors like Google and Amazon;
- virtualisation capabilities;
- commodity server hardware;
• open source software (e.g. Linux, Apache, and Hadoop), which has slashed the cost of software for data centres; and

• adoption of open Web 2.0 standards, which has made development of applications in the Cloud much easier and faster.

2.1 Types of Cloud Computing

There are four basic cloud delivery models, as outlined by NIST, which relate to who provides the cloud services. Agencies may employ one model or a combination of different models in delivery of applications and business services.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private or internal cloud</td>
<td>Cloud services are provided solely for an organisation and are managed by the organisation or a third party. These services may exist off site.</td>
</tr>
<tr>
<td>Community cloud</td>
<td>Cloud services are shared by several organisations and support a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). These services may be managed by the organisations or a third party and may exist off site. A special case of Community Cloud is the Government or G-Cloud. This type of cloud is provided by one or more agencies (service provider role), for use by all, or most, government agencies (user role).</td>
</tr>
<tr>
<td>Public cloud</td>
<td>Cloud services are available to the public and owned by an organisation selling cloud services, for example, Amazon.</td>
</tr>
<tr>
<td>Hybrid cloud</td>
<td>An integrated cloud services arrangement that includes a cloud model and something else (another cloud model, agency back end systems, etc.), e.g. data stored in private cloud or agency database is manipulated by a program running in the public cloud.</td>
</tr>
</tbody>
</table>

2.2 Cloud Service Capability

The Australian Government has adopted the three basic types of cloud service offerings, defined by NIST, and generally accepted by industry.

<table>
<thead>
<tr>
<th>Cloud Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software as a Service (SaaS)</td>
<td>Offers renting application functionality from a service provider rather than buying, installing and running software yourself. Examples include Salesforce.com and Gmail.</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td>Provides a platform in the cloud, upon which applications can be developed and executed. Examples include Salesforce.com, through Force.com, and Microsoft (Azure).</td>
</tr>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>Vendors offer computing power and storage space on demand. Examples include, Rackspace and Amazon S3.</td>
</tr>
</tbody>
</table>
2.3 Maturity of Cloud Computing

The Gartner Hype Cycle for Cloud Computing7 is illustrated below. As can be seen in the diagram, “cloud computing” is currently located at the peak of the hype cycle (at the peak of inflated expectations) with mainstream adoption predicted over the next 2 to 5 years.

However, the legal, contractual, economic and security aspects of cloud computing are still relatively immature, so agencies must exercise care in adopting this technology.
3 Drivers, risks and benefits

The drivers, risks and benefits of cloud computing have been adapted from the Cloud Computing Strategic Direction Paper – Opportunities and applicability for use by the Australian Government¹.

3.1 Drivers

Cloud computing advocates are claiming that cloud computing will transform the way IT is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand.

Some of the key drivers for agencies to adopt the cloud strategy include:

<table>
<thead>
<tr>
<th>Driver</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value for Money</td>
<td>• To reduce duplication and cost;</td>
</tr>
<tr>
<td></td>
<td>• Leveraging economies of scale;</td>
</tr>
<tr>
<td></td>
<td>• Increased savings through virtualisation;</td>
</tr>
<tr>
<td></td>
<td>• Allow for “measured” payment (pay as you use);</td>
</tr>
<tr>
<td></td>
<td>• Reduced energy use;</td>
</tr>
<tr>
<td></td>
<td>• Enable agencies to reinvest in, and concentrate on, core objectives;</td>
</tr>
<tr>
<td></td>
<td>• Adopt, where fit for purpose, modern technologies and practices that</td>
</tr>
<tr>
<td></td>
<td>improve ICT effectiveness and efficiency.</td>
</tr>
<tr>
<td>Flexibility</td>
<td>• Create a flexible services-oriented environment for agencies;</td>
</tr>
<tr>
<td></td>
<td>• Rapid provisioning and deployment of services and on demand scalability</td>
</tr>
<tr>
<td></td>
<td>and elasticity for services and capabilities.</td>
</tr>
<tr>
<td>Operational reliability</td>
<td>• High resiliency and availability;</td>
</tr>
<tr>
<td>/ robustness</td>
<td>• Standard offering.</td>
</tr>
</tbody>
</table>
3.2 Potential risks of cloud computing

As cloud computing is a new ICT sourcing and delivery model NOT a new technology, many of the risks and issues associated with cloud are also not new.

However, as most agency systems were designed to operate in a secure environment, agencies need to fully understand the risks associated with cloud computing both from an end-user and agency perspective and, based on this, adopt principle and risk-based approaches to their strategic planning.

Depending upon the cloud model adopted, an understanding and mitigation of the following issues will be required:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
</table>
| Application design     | • There may be less opportunity for customisation of applications and services. This may increase complexity when integrating cloud services with existing legacy environments;  
                          • Applications (could be either SaaS or Line of Business applications, etc.) will need to be treated at arms length from the infrastructure layer (IaaS);  
                          • Applications will need to be designed to accommodate latency; and  
                          • Existing software licensing models may not facilitate a cloud deployment. |
| Architecture           | • Moving to a cloud environment will require more emphasis on business design where cloud services will interface/impact business systems;  
                          • Prior to making a decision to move to a cloud computing environment, agencies must address the impact on business processes and eliminate any technical barriers; and  
                          • Finance recommends agencies use an architectural framework, such as the Australian Government Architectural framework (AGA) to assist in identifying potential opportunities to deliver common and shared cloud services across agencies. |
| Business continuity    | • Because the cloud is dependent on internet technologies, any internet service loss may interrupt cloud services;  
                          • Due to the dynamic nature of the cloud, information may not be immediately located in the event of a disaster; and  
                          • Business continuity and disaster recovery plans must be well documented and tested. |
| Data location and retrieval | • The dynamic nature of the cloud may result in confusion as to where information actually resides (or is transitioning through) at a given point in time;  
                              • When information retrieval is required, there may be... |
<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>delays impacting agencies that frequently submit to audits and inspections; and</td>
</tr>
<tr>
<td></td>
<td>• Due to the high availability nature of the cloud, there is potential for co-location of information assets with other cloud customers.</td>
</tr>
<tr>
<td>Funding model</td>
<td>• Due to the cloud’s pay-per-use model, some part of ICT capital budgeting will need to be translated into operating expenses (OPEX), as opposed to capital expenditure (CAPEX), which may have different levels of authorisations to commit expenses and procure services.</td>
</tr>
<tr>
<td>Legal &amp; regulatory</td>
<td>• Need to have the ability to discover information under common law;</td>
</tr>
<tr>
<td></td>
<td>• Need to be aware of Australian legislative and regulatory requirements including Archives Act, FOI Act and Privacy Act;</td>
</tr>
<tr>
<td></td>
<td>• Need to be aware of data sovereignty requirements;</td>
</tr>
<tr>
<td></td>
<td>• Need to be aware of legislative and regulatory requirements in other geographic regions, as compliance may be a challenge for agencies, for example, the US Government’s Patriot Act may become a key concern for data stored in the cloud and located within the United States; and</td>
</tr>
<tr>
<td></td>
<td>• Little legal precedent exists regarding liability in the cloud and because of this, service agreements need to specify those areas the cloud provider is responsible for.</td>
</tr>
<tr>
<td>Performance and</td>
<td>• Need to ensure that guaranteed service levels are achieved. This includes environments where multiple service providers are employed (e.g. combined agency and cloud environments). Examples include:</td>
</tr>
<tr>
<td>conformance</td>
<td>• Instances of slower performance when delivered via internet technologies;</td>
</tr>
<tr>
<td></td>
<td>• Applications may require modification;</td>
</tr>
<tr>
<td></td>
<td>• Monitoring and reporting are adequately delivered for the period between service introduction and exit; and</td>
</tr>
<tr>
<td></td>
<td>• Failure of service provider to perform to agreed-upon service levels.</td>
</tr>
<tr>
<td>Privacy</td>
<td>• Risk of compromise to confidential information through third party access to sensitive information. This can pose a significant threat to ensuring the protection of intellectual property (IP), and personal information.</td>
</tr>
<tr>
<td>Reputation</td>
<td>• Damage to an agency’s reputation resulting from a privacy or security breach, or a failure to deliver an</td>
</tr>
</tbody>
</table>
## Risk Description

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Description</td>
<td>essential service because risk was inadequately addressed must be considered for cloud computing applications.</td>
</tr>
</tbody>
</table>
| Skills requirements   | • A direct result of transitioning to a cloud environment means:  
                           • Less demand for hardware and system management software product-specific skills; and  
                           • More demand for business analysts, architects, portfolio and program and change managers, and vendor/contract managers. |
| Security              | • Must ensure cloud service providers and their service offerings meet the requirements of the Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM) and the Privacy Act 1988; and  
                           • With cloud computing, an agency may have limited ability to prescribe the protective security of the cloud environment. Yet agencies will remain ultimately responsible for the information that is stored and/or processed in the cloud. Management must maintain assurance that the security of the cloud service provider is in accordance with the PSPF. |
| Service provision     | • Reputation, history and sustainability should all be factors to consider when choosing a service provider;  
                           • Agencies should take into consideration the volatility of the growing cloud computing market; and  
                           • Agencies should ensure they address portability of data in the case of service provider failure. |
| Standards             | Strategies for open standards, interoperability, data portability, and use of commercial off the shelf (COTS) products are required for reducing the risk of vendor lock-in and inadequate data portability. Examples include:  
                           • Potential for inadvertent use of cloud services creating “islands” of cloud technologies that will reduce interoperability across cloud types and associated implementations;  
                           • A cloud provider decides to no longer stay in business, an agency’s data/application/processes must be able to be moved to another provider; and  
                           • Certification of projects by vendors for prescribed platforms and versions. |
### 3.4 Potential benefits of cloud computing

Transitioning to cloud services may offer the following business benefits for Australian Government agencies – the level of benefit will depend on the cloud model adopted.

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
</table>
| Scalability      | Unconstrained capacity allows for more agile enterprises that are scalable, flexible and responsive to change. For example:  
  - Faster responsiveness can benefit government service delivery, and meet the needs of citizens, businesses, employees, suppliers and corporate relations. For example, ability to provision and utilise a service in a single day;  
  - Option of scalability is provided without the serious financial commitments required for infrastructure purchase and maintenance; and  
  - Provisioning and implementation are undertaken on demand, allowing for traffic spikes and reducing the time to implement new services.  
  Agencies, however, need to be aware that when transitioning from legacy systems, data migration and change management can slow down the “on demand” adoption of cloud computing.                                                                                       |
| Efficiency       | Reallocation of IT operational activities offers opportunity for agencies to focus on:  
  - Research and development including new and innovative applications allowing for business and product growth (improved service delivery);  
  - Creating new solutions that were not technically and/or economically feasible without the use of cloud services;  
  - Enabling prototyping and market validation of new approaches much faster and less expensively;  
  - Providing the ability to de-couple applications from existing infrastructure; and  
  - Rationalising legacy systems.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Cost Containment | Changes to an agencies cost model can be modified by the following:  
  - Services and storage become available on demand without the serious financial commitments required for infrastructure purchase and maintenance. Additionally, they are priced as a pay-as-you-go service;  
  - Transfer of costs  
  - From CAPEX to OPEX  
    - no need to invest in high-cost IT equipment; for example, able to test software solutions without capital investment;                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◊ Reduction of operating costs</td>
</tr>
<tr>
<td></td>
<td>■ reduced energy consumption;</td>
</tr>
<tr>
<td></td>
<td>■ less expense in managing IT systems;</td>
</tr>
<tr>
<td></td>
<td>■ less cost and complexity in doing both routine computing tasks and computationally-intensive problems;</td>
</tr>
<tr>
<td></td>
<td>■ reduced associated with time delays;</td>
</tr>
<tr>
<td></td>
<td>■ potential to reduce support and maintenance costs through transitioning legacy systems to new systems;</td>
</tr>
<tr>
<td></td>
<td>■ potential to reduce the demand for data centre resources; and</td>
</tr>
<tr>
<td></td>
<td>■ potential to reduce the Government’s carbon footprint.</td>
</tr>
<tr>
<td></td>
<td>Note: agencies will need to compare current costs against potential cloud expenses and consider models for lowering total cost of ownership (TCO) to understand whether cloud services will offer any potential savings.</td>
</tr>
</tbody>
</table>

| Flexibility | • Agencies can save time at set-up, as cloud computing becomes functional faster than other systems;                                           |
|             | • To transition to the cloud, agencies are not required to install additional hardware or software;                                          |
|             | • Implementation can be undertaken remotely; and                                                                                           |
|             | • Potential to access latest technology through software applications being automatically updated by cloud providers.                       |

| Availability | • Cloud software architectures are designed from the bottom up for maximum network performance – potentially delivering improved application level availability than conventional IT solutions; and |
|              | • Greater flexibility and availability of ‘shared’ information enables collaboration from anywhere in the world – all that is required is an internet connection. |

| Resiliency   | • The potential for failure in a highly resilient computing environment is reduced. The failure of one node of a system in a cloud environment will have no impact on overall information availability and reducing the risk of perceivable downtime. |
5 Guidelines

This section outlines practical guidelines to consider when adopting public cloud computing solutions for their agency.

5.1 Tactical application

Tactical application and use of cloud by government at the Information and technology layers is illustrated in the diagram below.

It is possible now to move government data that is intended for public consumption or use to the public cloud.

Transitioning citizen (personal) information to the public cloud is not expected to be a viable option within the next several years until the security and privacy concerns are adequately addressed.

This is in contrast to the use of private and hybrid clouds, which represent more immediate or short term opportunities.

Decisions to transition at the information and services layers should be made based on a risk-managed approach taking into account information assurance requirements.

The content of the Data Centre with Advanced Virtualisation column represents a service provider view, while the content of the Private Cloud, Hybrid cloud, Community Cloud (Incl. G-Cloud) and Public Cloud columns represents a user view.

5.2 Three initial areas to test

The policy defines three areas which must be tested before implementing a public cloud computing solution for their agency. The policy is restated below (from section 1).

The Northern Territory Government (NTG) and its agencies may choose cloud based services if they demonstrate value for money and adequate security and privacy.

These three areas are value for money and adequate security and privacy.

5.2.1 Value for money test

Is the proposed cloud service provider’s solution value for money?
Agencies should satisfy themselves there is a clear business case before adopting a non-private cloud hosting solution for their requirements. Consideration of the NTG’s Data Centre (the NTG’s private cloud) should be considered as one of the options in their business case.

5.2.2 Security test

Is the security of the proposed service provider’s technical infrastructure sound?
What is the security level of the information you want to host?
What legal jurisdiction is the information subject to?

Security is of utmost importance and due consideration must be given to the level of infrastructure (technology) security provided by the cloud service provider and the security level of the information (content) itself.

There are restrictions on what information can be hosted in a public cloud environment as outlined in the Records Management Advice Number 10 – Cloud Computing and Record Keeping – June 2011.

There are 5 security levels for information defined in the Records Management Standards for Public Sector Organisations in the Northern Territory.

These are:
1. Unrestricted
2. NTG Restricted
3. In-confidence
4. Protected
5. Highly Protected

Information classified as “in-confidence” or above must not be hosted with a public cloud service provider.

Refer to Appendix 1 for a description of the relationship between the Information Act and the Records Management Standards for Public Sector Organisations in the Northern Territory and links to these documents.

5.2.3 Privacy test

Has your agency taken reasonable steps to protect personal information it holds?

Is your agency intending to transfer personal information outside the Northern Territory borders?

It is recommended agencies seek legal advice before hosting their information with a public cloud service provider.

An agency must ensure it is not breaching the Information Privacy Principles (IPPs) as prescribed in Schedule 2 of the Information Act. Refer to Appendix 2 for the IPPs from the Act.

For example, agencies should note IPP 4.1 and IPP 9.1. Agencies are held responsible under the Act to protect personal information and that this personal information does not flow outside the Northern Territory borders unless certain conditions are met.
IPP 4.1  “A public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure”

IPP 9.1  “A public sector organisation must not transfer personal information about an individual to a person (other than the individual) outside the Territory unless…” (refer to the full conditions)
5.3 Checklists

This section provides a checklist of further questions to consider. These have been adapted from Privacy Victoria.

1. When the additional steps required to ensure privacy protection are considered, is there an actual cost savings benefit to the government organisation?

2. Does the government organisation know exactly, geographically, where the data will be stored, keeping in mind the possibility it may be across different countries or continents?

3. Is the government organisation’s data segregated from other customers or government departments?

4. Who will have access to the data? How will system administrators or staff of the cloud service provider be prevented from unauthorised access to the data?

5. Does the service provider have methods of notification of, and responding to, data security breaches?

6. Does the contract permit the government organisation to audit the provider to ensure compliance with the Information Act?

7. Is the service provider owned or controlled by a foreign company? What control does the foreign company have over the service provider?

8. How will personal information be destroyed or retrieved when it is no longer needed, bearing in mind any requirements under the Information Act?

9. Is there data protection or privacy legislation in place in the foreign jurisdiction that at minimum meets the requirements in the Information Act? Is the relevant law enforceable?

10. Can the service provider guarantee that access will not be given to foreign governments or law enforcement? Is there a legislative requirement in that jurisdiction that prevents the Northern Territory Government organisation from being notified of any potential access?

11. What happens at the conclusion of the contract with the cloud service provider? Will information be able to be retrieved or destroyed in compliance with the Information Act?

12. What happens with the sale of business to another entity? A change of control may impact on contracts or obligations of the cloud service provider.

13. What is the risk of insolvency or bankruptcy to the service provider?

14. Are changes to business units or practices made without the knowledge of their IT units?

15. What happens with machinery of government changes?

16. What retrieval or destruction of information occurs once or if the contract with the cloud service provider terminates?
Appendix 1 – Information Act and Records Management Standards

The following diagram illustrates the relationship between the Information Act of the Northern Territory of Australia and the supporting Records Management Standards.

The Records Management Standards were issued in 2010 and were based on the Information Act 2009. The Information Act was updated in 2011 but has not affected the Records Management Standards of 2010.

Records Management Advices are issued from time to time and provide further detail to the Records Management Standards.

The following documents have also been referenced in the Reference section of this policy document, but for convenience are reproduced below.

1. **Information Act**
   
   NTG Legislation Database:
   

   Information Act:
   

2. **Records Management Standards**

Appendix 2 – Information Privacy Principles

Below are the Information Privacy Principles (IPPs) taken directly from the Information Act³

Schedule 2 Information Privacy Principles
Section 65(1)

IPP 1 Collection

1.1 A public sector organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 A public sector organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) a public sector organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that the individual is able to have access to the information; and

(c) the purpose for which the information is collected; and

(d) the persons or bodies, or classes of persons or bodies, to which the organisation usually discloses information of the same kind; and

(e) any law that requires the particular information to be collected; and

(f) any consequences for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, a public sector organisation must collect personal information about an individual only from the individual.

1.5 If a public sector organisation collects personal information about an individual from another person, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of the individual or another individual.

IPP 2 Use and disclosure

2.1 A public sector organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose for collecting it unless one or more of the following apply:

(a) if the information is sensitive information:

(i) the secondary purpose is directly related to the primary purpose; and
(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

(b) if the information is not sensitive information:

(i) the secondary purpose is related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

(c) the individual consents to the use or disclosure of the information;

(ca) the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest and the following apply:

(i) the research, compilation or analysis will not be published in a form that identifies the individual;

(ii) it is impracticable for the organisation to seek the individual's consent before the use or disclosure;

(iii) in the case of disclosure – the organisation reasonably believes the recipient of the information will not disclose the information;

(iv) if the information is health information – the use or disclosure is in accordance with guidelines issued by the Commissioner under section 86(1)(a)(iv) for this paragraph;

(d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to the individual's or another individual's life, health or safety; or

(ii) a serious or imminent threat of harm to, or exploitation of, a child; or

(iii) a serious threat to public health or public safety;

(e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in and uses or discloses the information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

(f) the use or disclosure is required or authorised by law;

(g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency:

(i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;

(ii) enforcing a law relating to the confiscation of proceeds of crime;

(iii) protecting public revenue;
(iv) preventing, detecting, investigating or remediing seriously improper conduct or prescribed conduct;

(v) preparing for or conducting proceedings before a court or tribunal or implementing the orders of a court or tribunal;

(h) the Australian Security Intelligence Organisation (ASIO) has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIO authorised by the Director-General of ASIO to receive the information and an officer or employee of ASIO authorised by the Director-General of ASIO to do so has certified in writing that the information is required in connection with the performance of the functions of ASIO;

(i) the Australian Secret Intelligence Service (ASIS) has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIS authorised by the Director-General of ASIS to receive the information and an officer or employee of ASIS authorised by the Director-General of ASIS to do so has certified in writing that the information is required in connection with the performance of the functions of ASIS.

Note 1: It is not intended to deter public sector organisations from lawfully co-operating with law enforcement agencies in the performance of their functions.

Note 2: IPP 2.1 does not override any existing legal obligations not to disclose personal information. IPP 2.1 does not require a public sector organisation to disclose personal information – a public sector organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: A public sector organisation is also liable to the requirements of IPP 9 if it transfers personal information to a person outside the Territory.

2.2 If a public sector organisation uses or discloses personal information under IPP 2.1(g), the organisation must make a written note of the use or disclosure.

2.3 In this IPP:

child, see section 13 of the Care and Protection of Children Act.

exploitation, see section 16 of the Care and Protection of Children Act.

harm, see section 15 of the Care and Protection of Children Act.

IPP 3 Data quality

3.1 A public sector organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.
IPP 4 Data security

4.1 A public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 A public sector organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

IPP 5 Openness

5.1 A public sector organisation must make available to the public a document in which it clearly expresses its policies for the management of personal information that it holds.

5.2 On the request of an individual, a public sector organisation must take reasonable steps to inform the individual of the kind of personal information it holds, why it holds the information and how it collects, holds, uses and discloses the information.

IPP 6 Access and correction

6.1 If an individual requests a public sector organisation holding personal information about the individual for access to the personal information, the organisation must provide the individual with access to the information except to the extent that:

(a) providing access would pose a serious threat to the life or health of the individual or another individual; or

(b) providing access would prejudice measures for the protection of the health or safety of the public; or

(c) providing access would unreasonably interfere with the privacy of another individual; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way that would prejudice the negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
providing access would be likely to prejudice one or more of the following by or on behalf of a law enforcement agency:

(i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
(ii) enforcing a law relating to the confiscation of proceeds of crime;
(iii) protecting public revenue;
(iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
(v) preparing for or conducting proceedings in a court or tribunal or implementing the orders of a court or tribunal; or

providing access would prejudice:

(i) the security or defence of the Commonwealth or a State or Territory of the Commonwealth; or
(ii) the maintenance of law and order in the Territory.

6.2 However, where providing access under IPP 6.1 would reveal evaluative information generated within a public sector organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than access to the decision.

6.3 If a public sector organisation holds personal information about an individual and the individual establishes that the information is not accurate, complete or up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.4 If:

(a) an individual and a public sector organisation disagree about whether personal information about the individual held by the organisation is accurate, complete or up to date; and
(b) the individual requests the organisation to associate with the information a statement to the effect that, in the individual's opinion, the information is inaccurate, incomplete or out of date;

the organisation must take reasonable steps to comply with that request.

6.5 A public sector organisation must provide reasons for refusing to provide access to or correct personal information.

6.6 If a public sector organisation charges a fee for providing access to personal information, the fee is not to be excessive.

6.7 If an individual requests a public sector organisation for access to or to correct personal information held by the organisation, the organisation must:
(a) provide access or reasons for refusing access; or
(b) make the correction or provide reasons for refusing to make it; or
(c) provide reasons for the delay in responding to the request;
within a reasonable time.

**IPP 7 Identifiers**

7.1. A public sector organisation must not assign unique identifiers to individuals unless it is necessary to enable the organisation to perform its functions efficiently.

7.2. A public sector organisation must not adopt a unique identifier of an individual that has been assigned by another public sector organisation unless:

(a) it is necessary to enable the organisation to perform its functions efficiently; or
(b) it has obtained the consent of the individual to do so; or
(c) it is an outsourcing organisation adopting the unique identifier created by a contract service provider in the performance of its obligations to the outsourcing organisation under a service contract.

7.3. A public sector organisation must not use or disclose a unique identifier assigned to an individual by another public sector organisation unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to that other organisation; or
(b) IPP 2.1(d), (e), (f) or (g) applies to the use or disclosure; or
(c) it has obtained the consent of the individual to the use or disclosure.

7.4. A public sector organisation must not require an individual to provide a unique identifier in order to obtain a service unless its provision:

(a) is required or authorised by law; or
(b) is in connection with the purpose for which the unique identifier was assigned or for a directly related purpose.

**IPP 8 Anonymity**

8.1. A public sector organisation must give an individual entering transactions with the organisation the option of not identifying himself or herself unless it is required by law or it is not practicable that the individual is not identified.

**IPP 9 Transborder data flows**

9.1. A public sector organisation must not transfer personal information about an individual to a person (other than the individual) outside the Territory unless:
(a) the transfer is required or authorised under a law of the Territory or the Commonwealth; or

(b) the organisation reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to these IPPs; or

(c) the individual consents to the transfer; or

(d) the transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual’s request; or

(e) the transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual; or

(f) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to the transfer;

(iii) it is likely that the individual would consent to the transfer; or

(g) the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred in a manner that is inconsistent with these IPPs.

IPP 10  Sensitive information

10.1 A public sector organisation must not collect sensitive information about an individual unless:

(a) the individual consents to the collection; or

(b) the organisation is required by law to collect the information; or

(c) the individual is:

(i) physically or legally incapable of giving consent to the collection; or

(ii) physically unable to communicate his or her consent to the collection;

and collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual; or

(d) collecting the information is necessary to establish, exercise or defend a legal or equitable claim.

10.2 Despite IPP 10.1, a public sector organisation may collect sensitive information about an individual if:

(a) the collection:
(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no other reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's
6 References


5 Northern Territory of Australia, June 2011. “Records Management Advice Number 10 – Cloud Computing and Record Keeping – June 2011” [online] Record Services, Department of Business, Northern Territory Government, viewed 30 June 2011,
