NSW Government

Cloud Services Policy and Guidelines

August 2013

CONTENTS

1. INTRODUCTION

The *NSW Government ICT Strategy* recognises that a strategic approach to the use of cloud-based services will provide opportunities to achieve better value ICT investment and improve service capability. Government's shift to a service orientation will take advantage of the increasing commoditisation of ICT and the rapidly developing cloud computing industry.

Public sector ICT investment is increasingly influenced by financial constraints, rapidly ageing technology and a higher standard of service delivery demanded by the community. Cloud services have the potential to address these challenges by improving the agility, scalability and reliability of ICT services and providing the agility to respond to changing business needs. This new approach to ICT sourcing and management will be critical to achieve value, drive innovation and support sustainable investment.

To progress the transition to a service orientation, NSW Government agencies will now be required to evaluate cloud-based services when undertaking ICT procurements to determine the ICT delivery model that provides the best value sustainable investment, taking account of the full range of cost-benefit considerations.

This document provides guidance to agencies in the decision making process by highlighting some of the key considerations when evaluating a cloud service. Not all government information assets or systems are appropriate for a cloud-based delivery model. However, consideration of required business outcomes, and the nature of agencies' applications, data and information assets, will determine the appropriate delivery model.

A number of other NSW Government initiatives support the adoption of ICT as a service, including streamlined procurement arrangements, standard contract terms and access to services through the data centre reform program.

The NSW Government has established an ICT Service Catalogue to provide an effective and efficient ICT supply chain providing agencies with easy access to services and pre-qualified vendors. Technical standards and policies that support common approaches, sharing and reuse of ICT services will be developed to help shape the offerings available on the Catalogue.

In collaboration with the ICT industry, the Procure IT Framework has been developed to provide a suite of standard documents, terms and conditions for ICT procurements. Further to this work, standard terms and conditions have been developed for as-a-service procurements. These will provide the necessary protections for agencies by ensuring responsibilities, such as those in relation to privacy and information management, are met, while allowing agencies to capture the benefits of new business models.

From the middle of 2013, data centre consolidation into two new NSW Government data centres will provide the opportunity for agencies to access ICT services from a range of providers, including 'data centre as a service' and other offerings. The Government data centres will also host a private government cloud to provide ICT services in a secure environment.

The NSW Government ICT Board is responsible for developing and maintaining ICT policies and guidelines for use across the public sector that will drive the transition to new ICT delivery models. This document will be reviewed and updated as necessary to account for evolving ICT offerings and agencies' needs.

1.1 Policy statement

The NSW Government has identified the adoption of cloud-based ICT services as a key factor in driving better value ICT investment and improving the agility, scalability and reliability of ICT services.

NSW Government agencies will evaluate cloud-based services when undertaking ICT procurements to determine the ICT delivery model that provides the best value sustainable investment, taking account of the full range of cost-benefit considerations.

Careful evaluation of an ICT delivery model is required for any solution, whether delivered through traditional in-house methods or cloud services. While not all government information or ICT will be suitable for cloud, where appropriate cloud services will support agencies' strategic transition to a service orientation.

1.2 Purpose

The Policy provides guidance for NSW Government agencies to determine which cloud delivery model is best suited to their business needs. This evaluation includes cost-benefit considerations, compliance and risk assessment.

Agencies can use the key considerations outlined in this policy as guidance in any review of cloud solutions which have already been implemented.

1.3 Scope

The Policy applies to all NSW Government Departments, Statutory Bodies and Shared Service Providers. The Policy does not apply to State Owned Corporations, however, it is commended for adoption.

1.4 Responsibility

All NSW public sector chief executives are responsible for ensuring that this policy is applied within their agency.

It is also recommended that compliance is regularly reviewed by each agency's Risk and Audit Committee. Oversight of the policy will be provided by the NSW Government ICT Board.

2. CLOUD SERVICES FOR NSW GOVERNMENT

2.1 Definition of cloud services

A cloud-based service provides on-demand delivery of ICT services over a network, commonly over the internet, from a shared pool of computing resources.

Cloud services are generally grouped into three types of offerings:

- Infrastructure as a Service (IaaS), where computing power, networking and storage is provided
- Platform as a Service (PaaS), where applications can be developed and executed
- Software as a Service (SaaS), where full application functionality is delivered.

These services are generally standardised and configured by the provider to maximise economies of scale, and are delivered through four basic models - private, public, hybrid and community cloud.

The differences relate to who provides the cloud services and how they are provided. Private cloud services are provided solely for the use of one organisation, and are managed by that organisation or a third party.

Public cloud services can be used concurrently by a number of unrelated users, while the hybrid model shares attributes of both private and public cloud models. An example would be data stored in a private cloud or agency database that is manipulated by a program running in the public cloud.

Community cloud services are shared by a number of organisations and support shared objectives, such as service delivery, security, policy, or compliance considerations.

2.2 Benefits of cloud services

Cloud-based ICT services provide opportunities for agencies to achieve better value, flexibility and reliability, and make sustainable service delivery improvements:

- **Cost** – Moving from customising and operating in-house ICT to using the best available 'off the shelf' commodity solutions will reduce the total cost of ownership. Flexible, on-demand services enable solution testing without significant capital investment and provide transparency of usage charges to drive behavioural changes within agencies.
- **Consumption based pricing** – The benefits of consumption based, pay-as-you-go pricing enables an agency to move to a model that is aligned to actual demand.
- **Agility** – On-demand, scalable and flexible services that can be implemented quickly provide agencies with the ability to respond to changing requirements and peak periods.
- **Innovation** – Innovation will be facilitated by rapid and continuous system development.
- **Resilience** – A large, highly resilient environment reduces the potential for system failure. The failure of one component of a cloud-based system will have less impact on overall service availability and reduce the risk of downtime.
- **Standardisation** – Adoption of cloud solutions by agencies will increase procurement of standard service offerings, providing opportunities for standardisation and improved interoperability.
- **In-built upgrades** – Future upgrades are removing the need for costly and lengthy upgrade cycles.

2.3 Data Centre Reform

The NSW Government data centres will provide reliable, secure and efficient 'data centre as a service' for agencies with in-house systems and infrastructure.

A private cloud will also be available from the data centres. This will give agencies an additional option to utilise private or public cloud services hosted in the service providers' data centres. Private government cloud hosted in the data centres will include IaaS, PaaS and SaaS, provided by third parties and government shared service providers, through the ICT service catalogue.

Private cloud services will be hosted in the data centres for the exclusive use of the government. These will provide required levels of security and connectivity and will expand and enhance data standardisation and sharing opportunities across government.

2.4 ICT service catalogue

The ICT service catalogue will provide an effective and efficient ICT supply chain that defines the essential characteristics of each service, including cost, to enable agencies to easily access ICT as a service, including cloud based solutions.

A range of ICT products and services are already available through the catalogue, which is accessed through the NSWBuy e-catalogues. The catalogue will be designed to be consistent with new sourcing strategies that meet government requirements and technical standards. Common approaches, technologies and systems will reduce unnecessary duplication, improve interoperability and provide better value.

2.5 Cloud pilot projects

A number of pilot projects are currently being examined by Government to better understand the implications of cloud based services. Preliminary outcomes of this reviewfrom the projects have already informed this policy, and the development of whole of government policies, contractual arrangements and the implementation of service offerings on the ICT service catalogue. Key areas being studied will include the technical, regulatory, cost, contractual, and usability aspects, the impact on the agencies involved and application for whole of government.

Evaluation of the pilot projects will continue until the end of 2013 and the outcomes will be used to update this policy document, as required.

Case studies will be developed to provide agencies and industry with concrete examples of government cloud service implementations.

3. EVALUATING CLOUD SERVICES

Evaluation of the opportunities provided by cloud services and particular delivery models will be undertaken by each agency in the context of their particular ICT portfolio and business needs. There are a number of key areas in an ICT portfolio that will determine which services will provide the best fit and value, while addressing security, privacy and other considerations.

These key areas include the nature of the applications and ICT services required, and the data and information that will be associated with those technologies. The evaluation of these considerations in relation to a specific business need, can guide the choice of options for cloud services and delivery models. When agencies are considering which delivery model best meets a business requirement, key questions in the decision process prompt the consideration of whether:

- the solution is available through a cloud delivery model
- applications or technologies are unique, specific to the agency, or can be replaced with generic services and amended business practices
- complex requirements for data and information management or critical operations are met (these may include accessibility, security, storage, retention and disposal considerations and would also require agencies to make decisions about privacy and information accessibility obligations)
- the requirements of a risk assessment, and if necessary a privacy impact assessment, can be met.

4. KEY CONSIDERATIONS

There are a number of key considerations in the evaluation of cloud based services. These will change over time as the ICT service catalogue is developed, new sourcing strategies are established and agencies have incorporated cloud based services into their ICT portfolios.

4.1 Cost-benefit

NSW Government agencies are required to conduct an economic appraisal as part of the capital investment process, including when investing in ICT. The economic evaluation of these services should include the total cost of ownership (TCO). The TCO assessment can consider and compare the full range of costs and benefits associated with various solutions. More information is provided on cost-benefit considerations in section 5 of this Policy.

4.2 Regulatory frameworks

NSW Government agencies are required to comply with a range of legislative frameworks concerning the security, privacy, access, storage, management, retention and disposal of government data and information. These frameworks must be carefully considered and factored into contract terms (see below). More information is provided in section 6.

4.3 Risk management

Risk management is to be undertaken in accordance with the agency's Risk Management Framework. More information regarding specific cloud related considerations is provided in section 7.

4.4 Contract terms

The *Procure IT Framework* is mandated for use by NSW Government agencies and provides a suite of standard documents, terms and conditions for ICT contracting. Modules of Procure IT version 3 will be developed with standard contract terms and conditions for as-a-service ICT models. A range of contract terms will need to be considered, depending on the nature of the data/information and type of cloud solution. More information on contract terms for cloud based services is provided in section 8.

4.5 Skills and capabilities

The migration to a new system, regardless of the delivery model, will require assessment of the agency's workforce capability. The skills and capabilities required to deploy ICT as a service with a cloud-based solution may decrease the demand for certain system maintenance/software skill sets, and increase the demand for business analysts, portfolio/program managers and vendor/contract managers.

There may also be implications for agency skills and capabilities requirements through the implementation of cloud services, for example, where 'commercial off-the-shelf' solutions are used and business practices need to be amended.

4.6 Change management

Further to capability considerations, agencies will need to consider the existing organisational environment when adopting new delivery models. The transition to an as-a-service model may have significant change implications. Moving to a cloud environment may require agencies to reconsider business design and enterprise architecture, particularly where cloud services interface with internal business processes and systems. This can impact capability requirements across the agency.

Adoption of a cloud service should be viewed as part of a larger business re-engineering project, rather than as a purely IT-related project. Early engagement across the agency on the change implications of transitioning to an as-a-service model will allow agencies to more easily take advantage of associated opportunities to improve business efficiency.

4.7 Technical considerations

The use of a cloud service will require consideration of specific technical requirements including LAN, WAN and bandwidth, security, compatibility with the various browser technologies, and implications for longer term data integration.

In order to achieve the levels of automation and virtualisation required in a cloud service, most providers offer a standard operating system with no, or limited, customisation. While improving cost effectiveness, this may increase complexity for agencies when integrating cloud services with legacy environments or with different cloud service providers.

A comprehensive assessment of the internal technical environment prior to implementation will contribute to a smoother migration, fewer unexpected costs and more timely delivery against project timeframes. While the effort, time and cost associated with remediating the internal technical environment may be high, it is an exercise that may need to be performed only once, after which the agency should be able to source additional cloud-based services more easily and more cost effectively.

4.8 Standards

Consideration of open standards, security, interoperability, and data portability are recommended in order to reduce the risk of technology lock-in and inadequate data portability. New sourcing strategies developed under the ICT Strategy and deployed through the ICT service catalogue will assist agencies in implementing suitable cloud-based arrangements.

4.9 Information management

NSW Government agencies will need to consider information management as a key element in the strategic planning and delivery of cloud services. Designing strategic approaches to cloud operations that meet corporate information management needs in simple and cost effective ways will deliver long term business and cost benefits.

Statutory responsibilities, information classification, business accountabilities and community expectations mean that various forms of information will need to be kept for periods ranging from 10 years to (in some cases) 100 years. Some State Records will be required to be stored indefinitely for archival purposes. Implementation of cloud arrangements requires an understanding of the sustainability required of the information, ie for long term and ongoing business, legal and community requirements. These considerations should be included in planning, monitoring, portability and export arrangements for government information.

Information in the cloud should be managed through internal controls with appropriate accountability arrangements. Management arrangements should include the routine purging of authorised time-expired business information, monitoring of high risk, long term value business information and the regular auditing of system operations.

5. COST-BENEFIT CONSIDERATIONS

Moving to a cloud delivery model will have implications for the cost-benefit assessment in the development of business cases.

5.1 Cost-benefit assessment

Agencies should evaluate the cost-benefit implications of cloud services through the policy and project evaluation framework provided by NSW Treasury. The cost-benefit analysis, including calculation of net present value (NPV), should include a full range of financial and economic impacts, along with the key benefits associated with cloud models.

Cloud and other 'as-a-service' offerings combine many indirect costs into a single service payment based on use. This means that there may be a wide range of financial implications for energy consumption, resourcing needs, data centre resources, capital costs for infrastructure and asset maintenance that need to be considered when comparing on-premises solutions with cloud services.

Key benefits associated with cloud based delivery models include:

- consuming ICT on demand and reducing the time needed to implement new services or address changing demand and peak periods
- remote implementation of computing resources, allowing quicker and automatic updates
- architecture created with the benefit of scale that delivers a defined level of security management, and the potential to reduce the likelihood of system failure.

5.2 Total cost of ownership

Agencies should also consider the total cost of ownership (TCO) when comparing cloud solutions with other delivery models. ICT investments are often characterised by significant and complex indirect costs. TCO facilitates analysis of the differences in costs and the impact of technologies and practices over multiple years.

A TCO assessment may include accounting for all the costs likely to be associated with an ICT investment over the economic life of the asset. These include capital, installation, operation, maintenance, software and upgrades, training, technical support, disposal and replacement costs. The cloud pilot project will examine these issues and inform the economic assessment of cloud based services.

5.3 Funding

Traditional delivery solutions are typically capital intensive, including a range of indirect costs, and require significant upfront funding along with ongoing depreciation. Cloud solutions are provided as a service and funded by recurrent operating expenditure, and do not typically require capital investment (as this is funded by the provider), unless, for example, the project includes capital for migration. The cloud model packages into the service cost many of the indirect costs associated with ICT investment, and may increase the apparent cash flow requirements for day to day operations.

Agencies will need to consider the implications of this transition from capital to operating expenditure, which will impact on the value of assets and therefore the agency's overall balance sheet.

5.4 Asset impact

Traditional ICT service delivery assumes the retention of an asset that has a tangible value. This impacts the financial management of the asset and the assumed value of the organisation.

Where agencies have existing licence agreements in place, consideration needs to be given to whether those licences can be leveraged and any potential cost impacts when they expire.

5.5 Organisational impact

Business case development should include an analysis and impact assessment of a range of costs associated with the change to a new delivery model for ICT. This may include the potential disruption to the skills requirements of ICT staff and account for re-training or recruitment of key skills.

Considerations of information-related costs when moving to a cloud service delivery model may include:

- moving information into or out of cloud systems
- data cleansing associated with migration
- loss of functionality, capacities and metadata that could come from moving to a more generic and less business-specific operating environment.

The TCO assessment should consider these costs and compare them against alternative solutions.

5.6 Technical environment

With the move to cloud based solutions there may be increased traffic along organisational (LAN and WAN) networks. As with any business case, costs incurred to improve or expand the capacity of the required underlying infrastructure will need to be taken into account. Cloud delivered solutions may have a larger impact on existing networks than traditional delivery models.

Business case development should include an impact analysis on existing networks and identify the costs and dependencies of any required improvements. The TCO assessment should consider these costs and compare them against alternative solutions.

6. NSW REGULATORY FRAMEWORK

The primary instruments regulating the collection, storage, access, use and disclosure of data by NSW public sector agencies are:

- *State Records Act 1998:* regulates the creation, management and protection of the records of public offices and provides for public access to those records.
- *Privacy and Personal Information Protection Act 1998* (PPIPA)*:* provides for the protection of personal information and contains obligations in relation to storage, access, use and disclosure.
- *Health Records and Information Privacy Act 2002* (HRIPA)*:* health information is excluded from the operation of the PPIPA but is specifically protected under the HRIPA, which contains 15 health privacy principles that prescribe what organisations must do when they collect, hold, use or disclose health information.
- *Government Information (Public Access) Act 2009* (GIPAA)*:* gives members of the public an enforceable right to access government information.
- Premier's Memorandum M2012-15 *Digital Information Security Policy*: provides for compliance with relevant security standards and for the development of electronic information security management systems within agencies, including the specification of core requirements for agencies.

Many other legislative instruments regulate public sector data. These include:

- *Evidence Act 1995*
- *Electronic Transactions Act 2000*
- *Ombudsman Act 1974*
- *Public Finance and Audit Act 1983*
- *Independent Commission Against Corruption Act 1988*
- *Public Interest Disclosures Act 1994*
- *Crimes Act 1900.*

Public sector agencies must also bear in mind Parliament's powers to compel production of records under the NSW Constitution and Standing Orders.

6.1 Information and records management

The *State Records Act 1998* is the primary instrument in relation to the creation, management, protection and on-going accessibility of records of public offices in NSW. The Act outlines requirements that ensure good governance, use and management of records. It currently requires that a State record must not be taken or sent outside NSW unless authorised by the State Records Authority. A General Authority (GA35) for transferring records out of NSW for storage with or maintenance by service providers based outside of the State was made under section 21(2)c of the Act to address the movement of State records into remote cloud environments.

Under the General Disposal Authority sending records for storage with, or maintenance by, service providers based outside NSW is allowed, provided that an appropriate risk assessment has been made and that the records are managed in accordance with all the requirements applicable to State records under the State Records Act. In particular, public offices must:

- assess and address the risks involved in taking and sending records out of the State for storage with or maintenance by service providers based outside of NSW
- ensure the service providers facilities and services conform to requirements in standards issued by State Records Authority

- ensure contractual arrangements and controls are in place to ensure the safe custody and proper preservation of records
- ensure that the ownership of the records remains with the public office
- monitor the arrangement to ensure the service provider is meeting relevant requirements.

The General Disposal Authority provides authorisation for taking and sending records out of the State in terms of the State Records Act only and, as noted above, there are other legislative obligations in regards to certain types of records that may need to be taken into consideration.

Further information is provided on the State Records Authority website and in the *Recordkeeping in Brief - Storage of State records with service providers outside of NSW (RIB54).*

Care must be taken not to take or send records out of the State in contravention of any legal responsibilities or business interests the agency may have. Part of the risk assessment should involve the identification of all statutory or other limitations on their actions.

6.2 Information privacy

The collection, storage, access, use and disclosure of personal information is governed by the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*.

Where the use of cloud computing requires the transmission or storage of personal information, Government agencies must ensure that their arrangements comply with relevant privacy and disclosure requirements.

Under the Acts mentioned above, an agency must not do anything, or engage in any practice, that contravenes an Information Protection Principle applying to the agency. Particular areas of cloud services which may impact data privacy include:

- disclosure of personal information to a cloud service provider
- data security and safeguards against misuse or loss, unauthorised access, use, or alteration
- ensuring ongoing accessibility for the agency and data subject
- legislative environment and governing data laws in the location where data is stored
- determining who has control of data at the end of a contract
- authorised data retention and disposal.

If an agency shares or transfers personal information with a contracted cloud service provider and the cloud service provider simply holds the data and acts according to the instructions of the agency, then disclosure will not be considered to have occurred. If the cloud service provider uses the data provided for its own purposes, this may be unauthorised access, use, modification or disclosure.

Agencies must ensure that contractual arrangements with a cloud service provider explicitly address this, and take such security safeguards as are reasonable in the circumstances to prevent authorised access or use. These arrangements will need to take into account circumstances that may include where one or more functions of an agency are outsourced to a provider, or where a cloud service provider is asked to perform some action on the personal information which they had previously only been storing.

Agencies should refer to their Privacy Management Plan and use the checklist available from the Information and Privacy Commission website to identify privacy issues associated with proposed cloud services solutions.

6.3 Information access

The *Government Information (Public Access) Act 2009* gives members of the public an enforceable right to access government information.

Issues to be considered in relation to information access include:

- Is agency access to data guaranteed?
- Can eligible third parties (such as individuals to whom the data relates or regulators monitoring compliance with statutory regulation) access data?
- Can the agency audit data access?
- How will system administrators or staff of the cloud service provider be prevented from unauthorised access to the data?

Agencies must ensure that records and data created, stored or managed in the cloud remain accessible and retrievable in order meet GIPAA and other regulatory requirements for information access.

6.4 Information security

The NSW Government's *Digital Information Security Policy* (M2012-15) establishes the digital information security requirements for the NSW public sector, including the requirement to have an Information Security Management System (ISMS) that demonstrates compliance with a minimum set of controls, and requirements relating to certification, attestation and the nomination of Senior Responsible Officers to a Digital Information Security Community of Practice.

Agencies will need to ensure that any cloud-based service will comply with the agency's ISMS.

7. RISK ASSESSMENT

NSW Government agencies are required to undertake a comprehensive risk assessment in relation to the storage and maintenance of public sector information and records by a cloud provider. It is recognised that there will be some classifications of government information that may be unsuitable for cloud-based services.

As cloud computing is a new ICT delivery model rather than a new technology, many of the risks and issues associated with cloud are similar to those for existing delivery options. As agencies evaluate different delivery options for ICT, the assessment of the risk profiles will be required for the various cloud options compared with traditional in-house models. This decision making process will also include determining the agency's capability for the adoption of new delivery models.

Currently, agency systems are designed to operate in a well-defined environmental perimeter that is assumed to be secure. A full understanding of the risks, as well as opportunities, associated with 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.

NSW Government agencies evaluation of cloud computing options must appropriately address all identified risks and must take account of:

- *NSW Treasury Policy & Guidelines Paper TPP09-05 - Internal Audit and Risk Management Policy for the NSW Public Sector*
- *AS/NZS ISO 31000 Risk management - Principles and guidelines*
- *NSW Government Digital Information Security Policy*.

Depending upon the service type, business need and delivery model adopted, an understanding and mitigation of risks will be required, including, but not limited to:

- **Business continuity** - As with all ICT delivery options, business continuity and disaster recovery plans must be well documented and tested.
- **Data location and retrieval** – Data residence and sovereignty needs to be understood and implications managed.
- **Legal and regulatory** - There is still only an emerging understanding of legal risks and issues surrounding cloud, with little legal precedent and many untested areas.
- **Information governance and management** – Agencies must ensure cloud service providers and their service offerings comply with all applicable NSW information management frameworks.
- **Privacy** - Agencies must ensure cloud service providers and their service offerings meet all applicable NSW and Australian legislative requirements relating to the privacy of information.
- **Security** - Agencies must ensure cloud service providers and their service offerings meet all applicable NSW and Australian legislative requirements relating to the security of information.
- **Licensing** - Existing software licensing models may not seamlessly translate to a cloud deployment solution.

8. CONTRACT TERMS

It is recommended agencies develop a sound understanding of the fundamental issues to be addressed in cloud services contracts. This may assist with the evaluation of suppliers. It will also ensure the final agreement meets business needs, compliance requirements and minimises any risks associated with the solution.

8.1 Procurement requirements

The *Procure IT Framework* provides a mandatory suite of standard documents, terms and conditions for ICT contracting for NSW Government agencies. Modules of Procure IT version 3 are being developed with standard contract terms and conditions for as-a-service ICT models. Over time, as new modules are developed and as-a-service offerings defined, more detailed consideration will be given to contracting terms around cloud options.

In the meantime, NSW public agencies should ensure that contract terms support their ability to meet legal, regulatory and service delivery requirements.

It is the responsibility of agencies to undertake risk assessment, due diligence and privacy impact assessments to ensure compliance with the current legislative framework. Specific issues will be identified by agencies through the compliance and risk assessment processes, according to the type of service and delivery model that best meets the agency requirements and risk profile.

8.2 Key provisions

Contract terms are an important means of ensuring an agency retains sufficient control over its data to meet a range of regulatory obligations, and to ensure a provider is legally bound to meet the agency's instructions.

The following are the key areas that agencies must consider when entering into contractual arrangements, including, but not limited to:

Custody and ownership

While evaluating or negotiating cloud services, public sector agencies must ensure that NSW Government retains ownership of its information assets.

Contractual provisions should:

- explicitly state that the public agency is the owner of all rights, title and interest in the data and that all data will be maintained, backed up and secured until returned on termination of the agreement (unless other provisions are made for the migration, transfer or destruction of the data)
- identify the actual geographic locations where data storage and processing will occur
- confirm the jurisdiction which governs the operation of the contract, and application of privacy, confidentiality, access and information management laws
- confine data storage and processing to specified locations where the regulatory framework and technical infrastructure allow the public agency to maintain adequate control over the data.

Security, privacy and access

It is essential that any engagement with a cloud service provider guarantees the security of data and provides for notification of breaches. Legislation also requires agencies to maintain control over the accessibility of their data.

Contractual provisions to consider:

- Specific security standards with which the provider must demonstrate compliance, including a warranty in relation to security, related storage and access obligations, and service level agreements that include cost and operating requirements of providing service continuation in business critical

and non-business critical services when disruptions arise.

- Prescribe the security provisions the service provider must implement, consistent with the *NSW Government Digital Information Security Policy*, for example, where required, certified compliance with *AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems* or equivalent.
- Prohibit any unauthorised access, use or alteration of the data. Document the technical mechanisms and procedures in place to support this restriction (for example: agency control of user credentials for authentication; data encryption; information dispersal; data separation and segregation). Ensure that the contract prevents unauthorised access or use by the service provider or sub-contractor, including any 'third party use' of data.
- The computing processes by which the cloud service provider secures its information and the encryption between agencies and any overseas cloud storage location should be investigated and guaranteed by contractual terms.
- Contractual arrangements should allow agencies to receive data breach notifications.
- The security obligations imposed by the agreement on the cloud service provider should include the terms of the provider's Information Security Management System.
- Specify that that any personal information contained in the data is subject to PPIPA, HRIPA and any other relevant legislation, as applicable. This would include that any person or body providing data services (relating to the collection, processing, disclosure or use of personal information) for, or on behalf of, a public sector agency must abide by the Information Protection Principles.
- State that the agency retains an immediate and ongoing right of access to all agency data held by the cloud service provider.

Include provisions allowing auditing of the data or the service to ensure agencies meet their requirements under policy and legislative frameworks.

Business continuity, data disposal and exit strategy

Agencies must be able to guarantee the accuracy, integrity and reliability of data to ensure the ongoing availability of the data and maintain control over its retention or disposal. Agencies should also have a contingency plan to migrate data securely to another solution or provider or agency – which may be required in a range of different scenarios.

Contractual provisions to consider:

- Document the technical mechanisms and procedures that prevent data loss (for example: contractor/agency responsibilities and routines for backup, failover or redundancy).
- Provisions for continuity of accessibility, usability and preservation of all agency data regardless of any migration of data to other formats during the contract. Terms should provide for appropriate testing to ensure data integrity prior to any migration.
- Specify provisions and procedures for backup, restoration of services and disaster recovery.
- Upon transfer of data, ensure technological parity with other service providers is guaranteed.
- Contractual arrangements should guarantee the preservation of data and provide for routine monitoring of data in order to identify formats that are at risk of obsolescence.
- Contractual arrangements should include provisions relating to migration of data to new formats when appropriate and the provision of proper documentation about migration activities to the agency.
- Include provisions for the safe return/transfer of data should the cloud service provider be the subject of a takeover.
- At the termination of the agreement with a cloud service provider, specify what will happen to the

data (for example: transferred to a new provider; returned to the agency; permanently deleted).

- Specify remedies for service provider mistakes or breaches.
- Identify any penalty provisions imposed by the service provider (for example: suspension of agency access to data for non-payment).
- Define contract provisions relating to migration of data on termination of the contract.
- Precise terms for the disposal of specific data (a) during the term, at the request of the agency; and (b) at the end of the term, including a warranty in relation to technological parity/obsolescence.
- Limit any suspension and termination rights available to the cloud service provider.
- Subscription levels should be scalable up and down according to demand.
- Reporting and audit rights of the client and vendor should be contractually explicit.

9. DOCUMENT CONTROL

9.1 Document history

Status: Draft

Version: 1.1

Approved by:

Approved on:

Issued by:

Contact: John Thomas, Director, ICT Services, ICT Policy, Department of Finance and Services

Email: John.Thomas@services.nsw.gov.au

Telephone: (02) 9372 8286

9.2 Review date

This policy will be reviewed in 12 months. It may be reviewed earlier in response to post-implementation feedback from Departments.