

Cloud computing

Agencies are to use computing solutions that best meet business requirements having due regard to:

- **benefits and value**
- **risks and mitigations**
- **protections and controls.**

18 September 2017
Version 2.1

Contents

1	Policy statement.....	4
2	Purpose.....	4
3	Definitions.....	4
3.1	Cloud computing.....	4
3.2	External cloud service.....	5
3.3	NTG cloud service	5
4	Assessment of cloud computing services	6
4.1	Chief Executive certification	6
4.2	Risk assessment.....	6
4.3	Risk mitigation	7
4.4	Re-use of existing services	7
4.5	Use of NTG cloud service	7
5	Privacy requirements	8
5.1	Personal information	8
5.2	Privacy and confidentiality.....	8
6	Security requirements.....	9
6.1	Data security.....	9
6.2	NTG ICT Security assessment.....	9
6.3	Certified cloud service list	10
6.4	Security accreditation.....	10
6.5	Security classification of information	11
6.6	Security measures for information classified “in confidence” or above	11
6.7	Authentication	11
7	Administrative requirements	12
7.1	Agency access.....	12
7.2	Data ownership.....	12
7.3	Data sovereignty.....	12
7.4	Records management and Freedom of Information	12
7.5	Audit	13
8	Procurement and contract management requirements.....	13
8.1	Procurement	13
8.2	Contracts	13
8.3	Legal review and advice	14
8.4	Costs	14
8.5	Liabilities and indemnities	14
8.6	Contractor performance management	14
8.7	Subcontractors.....	15
8.8	Termination rights and transition-out provisions	15
8.9	Change of control	16
8.10	Periodic review	16
9	Other requirements	17

9.1	Key stakeholder acceptance	17
9.2	Community	17
10	External cloud services register.....	17
10.1	Maintain register	17
10.2	Allocate responsibility	18
11	Glossary of acronyms	18
12	Supporting references	18
12.1	NTG documents.....	18
12.2	Australian Government documents	18
	Appendix A: External Cloud Service proposal	20
	Appendix B: Flowchart	21
	Appendix C: Flowchart (as text)	22
13	Document control.....	24

Authority

Cloud computing policy

Information Act (including Schedule 2: Information privacy principles)

Treasurer's directions ICT 1.2 ICT policies and standards

1 Policy statement

Agencies are to use computing solutions that best meet business requirements having due regard to:

- benefits and value
- risks and mitigations
- protections and controls.

2 Purpose

This standard specifies the accountability requirements and controls for cloud computing. This standard is to be read in conjunction with the **Cloud Computing Policy** and all other relevant laws and government regulations, policies or procedures listed in section 12.

3 Definitions

3.1 Cloud computing

- The NTG has adopted the definition of “cloud computing” used by the Australian Government. This in turn is adopted from the US Government’s National Institute of Standards and Technology (NIST) Definition of cloud computing, which may be viewed in full at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.
- In summary, cloud computing is a model for enabling convenient, on-demand network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, website hosting and services) that can be rapidly accessed with minimal management effort or service provider interaction.

3.1.1 Essential characteristics

- The five essential characteristics of cloud computing are:
 - on-demand self-service – a consumer can access computing capabilities (e.g. server time and network storage), as needed automatically
 - broad network access – capabilities are available over the network and accessed through standard devices (e.g., mobile phones, tablets, laptops, and workstations)
 - resource pooling – the provider’s computing resources (e.g. storage, processing, memory, and network bandwidth) are pooled to serve multiple consumers
 - scalability on demand – capabilities provided to the consumer can be rapidly increased or decreased to meet demand
 - measured service – cloud systems automatically control and optimize resource use through usage metering and reporting, providing transparency for the provider and consumer.

3.1.2 Service models

- i. The three main cloud computing service models are:
 - a) Software as a service – provision of software over a network rather than the software being loaded directly onto a locally available computer (for example, business applications and website hosting)
 - b) Platform as a service – provision of computing platforms that create the environment for other software to run (for example, operating systems) over a network rather than being loaded directly onto a locally available computer
 - c) Infrastructure as a service – provision of access to computer infrastructure (for example, data storage or processing capability) over a network that is used to complement local platform resources.

3.1.3 Deployment models

- i. The four cloud computing deployment models are:
 - a) Private cloud – use of the cloud infrastructure is restricted to a single organization comprising multiple consumers (for example, a single agency)
 - b) Community cloud – the cloud infrastructure is used by a specific community of consumers from organisations that have shared concerns (for example, a range of government agencies)
 - c) Public cloud – the cloud infrastructure is used by the general public
 - d) Hybrid cloud – a composition of two or more of the above models, bound together by technology that enables them to operate interactively (i.e. by enabling data and application portability).

3.2 External cloud service

- i. For the purposes of this standard and the related policy, an external cloud service is any model which fits the definition of cloud computing in section 3.1, and which is not an NTG cloud service. This includes public and community cloud deployment models, as well as private deployment where the owner, manager or operator is a third party and not the NTG, and any hybrid of these models.

3.3 NTG cloud service

- i. For the purposes of this standard and the related Policy, an **NTG cloud service** is a cloud computing service hosted within the NTG ICT environment and owned, managed and operated solely by the NTG. For example, cloud computing services provided by the NTG's Data Centre Services, such as data storage and backup services for NTG agencies and website hosting.

4 Assessment of cloud computing services

4.1 Chief executive certification

- 4.1.1.1 Agency chief executives must decide the computing service solution that best meets the agency's business needs having considered appropriate due diligence investigations by the agency.**
- 4.1.1.2 Agency chief executives must assure themselves that the controls specified in the Cloud computing policy and standard are met and will continue to be met for the duration of the arrangement with the cloud service provider.**

- i. Responsibility for the decision to adopt an external cloud service rests with the agency chief executive, who must be satisfied, on the basis of a thorough due diligence investigation including a risk assessment, that the relevant service provides appropriate data privacy, security, business benefits, continuity and value for money.
- ii. Copies of the risk assessment required under section 4 of this standard, the assessment or advice from NTG ICT Security, required under section 6.2, and the assessment or advice of Privacy Requirements required under section 5 are to be provided to the agency chief executive to assist in making the decision.
- iii. The above requirements apply regardless of the cost of the external cloud service and in each instance an agency function is being considered for transition to or establishment with an external cloud service provider, including consideration of changing between external providers.
- iv. A checklist is included in Appendix A to assist the agency chief executive in identifying assessment elements and documentation needed to make an informed decision.

4.2 Risk assessment

- 4.2.1.1 Agencies must undertake a detailed risk assessment before commencing a project to establish or transfer to an external cloud services provider in accordance with the ICT project requirements set out in the Treasurer's directions.**

- i. Where agencies are making substantial business decisions and particularly where control of NTG information and processes is being considered to move to an external entity, a full assessment of the risks is necessary. NTG agencies have a responsibility to the community and a duty of care to their clients to protect client data and to deliver reliable and suitable government services. Agency clients and the community expect government to manage and will hold the NTG to account for the quality of service delivery, including data protection; irrespective of the methods agencies employ for this purpose.
- ii. Agencies need to fully understand the risks and benefits with external cloud computing from an end-user, agency and NTG perspective.
- iii. This risk assessment is to be documented and provided to the agency chief executive to consider in providing certification under section 4.1 of this standard and recorded in the external cloud services register under section 10.

4.3 Risk mitigation

4.3.1.1 Agencies must consider and implement appropriate mitigations to reduce or eliminate the likelihood and/or impact of identified risks.

- i. Where the risk assessment at 4.2 results in the agency considering that use of the cloud services provider remains appropriate in their circumstances, the agency must develop, document and implement mitigation actions that will reduce or contain the identified risks to levels that are acceptable to the agency.

4.4 Re-use of existing services

4.4.1.1 Agencies must maximise common solutions and processes through sourcing ICT solutions that service the needs of all or multiple agencies and the community (Treasurer's direction ICT 1.3.2 refers).

- i. Agencies share ICT similarities across government and reusing or sharing of solutions is the default position. Standardisation for any major investments in ICT systems is required unless the agency has unique or specialised business needs.
- ii. Agencies can leverage existing external cloud services provided to other agencies to obtain better value for government, where the services are suitable and the risk assessment supports this approach.

4.5 Use of NTG cloud service

4.5.1.1 Agencies must give due consideration to use of the NTG cloud service as a computing service solution.

- i. The NTG cloud service operates within the NTG ICT environment, within its firewalls, and the data centres at which information is stored are located in the Northern Territory and owned by the NTG. As information is stored on premise, the NTG has a far greater degree of control over information stored in the NTG cloud service, with known standards of data governance and confidentiality.
- ii. The NTG cloud service is simpler from legal and contractual perspectives with surety of control and no commercial risk.
- iii. Integration and effective operation within and across the NTG's ICT network is delivered with this service.

5 Privacy requirements

5.1 Personal information

5.1.1.1 Agencies must consult the information commissioner or seek legal advice where personal information is proposed to be stored with an external cloud services provider.

- i. The Northern Territory *Information Act* regulates the collection, use and storage of personal information by public sector organisations. Schedule 2 of the *Information Act* prescribes information privacy principles (IPPs) that regulate the manner in which personal information may be dealt with, including obligations to protect and access personal information, and limitations on the trans-border data flow of personal information.
- ii. “Personal information” is defined as government information that discloses a person's identity or from which a person's identity is reasonably ascertainable.¹

5.1.1.2 Agencies must consider and implement appropriate mitigation actions to address risks relevant to data privacy.

- i. The privacy assessment or advice should be undertaken at the earliest possible opportunity.

5.2 Privacy and confidentiality

5.2.1.1 Agencies must ensure that arrangements with the external cloud service provider comply with the privacy requirements of the *Information Act* (NT).

- i. More generally across all the data proposed to be held with an external cloud services provider, the agency is certain that:
 - a) the arrangement with the service provider will support and enable compliance with any obligations (whether contractual, equitable or statutory) on the agency to keep particular information confidential
 - b) such confidentiality obligations are transmitted to the service provider in circumstances where the provider is storing or accessing the agency's data.

¹ *Information Act* (NT) s 4A

6 Security requirements

6.1 Data security

- 6.1.1.1 Agencies must protect data that belongs to the NTG or is entrusted to the NTG on behalf of clients, citizens and businesses.**
- 6.1.1.2 Agencies must ensure that government data in a cloud service is secure and protected where this is necessary.**
- 6.1.1.3 Agencies must ensure that contractual arrangements with the external cloud services provider provide for adequate data protection and security over the contract term and beyond.**

- i. For this standard, data refers to data that is collected by agencies and held in digital form that is being considered for hosting or storage with a cloud services provider.
- ii. ICT and data security is of utmost importance and agencies must give due consideration to the level of infrastructure (technology) security provided by an external cloud service and the security level of the information (content) proposed to be hosted in the external cloud service.
- iii. Agencies must have a clear understanding of the nature of the information proposed to be stored in the external cloud service; have attributed an appropriate security classification level to the information; and implemented security controls commensurate with the classification level.
- iv. Arrangements must be in place to provide certainty that:
 - a) agency data stored off-premises is protected from potential threats (such as security breaches or introduction of harmful code) at all times and for as long as the external cloud service is provided by the provider
 - b) the security standards (e.g. configurations, protocols, etc.) used by the service provider are acceptable to the NTG and that the service provider will be bound to maintain such standards for the duration of the contract.
- v. Where the government data is 'open' (publicly available) the contractual arrangements can be adjusted to suit, provided that the NTG's reputation and obligations to third parties remain adequately protected at all times.

6.2 NTG ICT Security assessment

- 6.2.1.1 Agencies must submit all proposals for use of external cloud services, regardless of value, to NTG ICT Security for assessment prior to commencement.**

- i. In addition to protection of data and evaluation of the adequacy of ICT security measures employed by an external cloud services provider; it is essential that the security and integrity of the broader NTG ICT environment, including government networks and devices, is maintained at all times.

6.2.1.2 NTG ICT Security will assist agencies to assess cloud offerings in all areas of security. NTG ICT Security must assess the potential for use of an external cloud service to introduce vulnerabilities into the NTG ICT environment or expose the environment to potentially harmful cyber threats.

6.2.1.3 NTG ICT Security must advise agencies of security controls and requirements.

- i. If the external cloud service fails the security assessment, it may be prohibited and denied access to the NTG ICT environment. It is recommended that agencies seek the advice of NTG ICT Security at the earliest possible opportunity.
- ii. NTG ICT Security can assist agencies by informing of appropriate solutions and ways to satisfy security requirements where this is feasible.

6.3 Certified cloud service list

6.3.1.1 Agencies are to consult the Australian Government's certified cloud services list and give priority to certified cloud services providers.

- i. The Australian Signals Directorate (ASD) within the Australian Government maintains a certified cloud services list (CCSL). Providers included on this list have satisfied ASD IRAP security assessments and requirements stated in the Australian Government's information security manual.
- ii. This will provide greater assurance when NTG ICT Security assesses the cloud service.
- iii. Where an agency intends to use an external cloud services provider not on ASD's CCSL, the agency is to take additional precautions and undertake further due diligence, including attention to compliance with the *Information Act* and to where the provider is located (Australia or overseas).
- iv. The CCSL is accessible at http://www.asd.gov.au/infosec/irap/certified_clouds.htm.

6.4 Security accreditation

6.4.1.1 Agencies must obtain written confirmation of the external cloud services provider's security accreditation.

- i. The physical data centre to store the agency's information, and the provider's internal controls should be assessed and accredited by a registered information security registered assessors program (IRAP) assessor.
- ii. Where the external cloud service provider's security accreditation has already been determined and assessed, such as by the Australian Government and the provider is recorded on the certified cloud services list, a further assessment is not required.
- iii. If an IRAP is not available or accreditation is not known, evidence of assessment against an appropriate industry standard must be submitted by the external cloud services provider, including evidence of independent verification. This documentation must be reviewed by NTG ICT Security to determine the suitability of the provider's security controls.

6.5 Security classification of information

6.5.1.1 Agencies must ensure that the security level of information proposed to be stored in an external cloud service is assessed and a security classification attributed, having regard to requirements of the records management standards.

- i. There are five security levels for information defined in the records management standards for public sector organisations in the Northern Territory:
 - a) unrestricted
 - b) NTG Restricted
 - c) in-confidence
 - d) protected
 - e) highly protected.

6.6 Security measures for information classified “in confidence” or above

6.6.1.1 Agencies must consult NTG ICT Security where proposing to put information classified as ‘in confidence’ or above in an external cloud service solution.

6.6.1.2 NTG ICT Security must assess such agency requests in further detail and determine additional security measures required to mitigate risks.

- i. Agencies should be particularly cautious about hosting and storing information classified as “in-confidence” or above with an external cloud service, given the increased legal and reputational risks which may arise if such information is not kept appropriately secure.
- ii. If information classified as “in-confidence” or above is to be hosted by an external cloud service, agencies will be required to establish and maintain additional security measures, including virtual private networks and multifactor authentication.
- iii. NTG ICT Security will evaluate and determine the additional security measures that are necessary.

6.7 Authentication

6.7.1.1 Agencies must consult NTG ICT Security to ensure that the external cloud service provider uses approved authentication processes to control access, or where a federated environment is required.

- i. Local authentication compromises NTG security and external cloud services should not be accessible to users through local authentication. That is, the service should not ask users to create specific authentication details (usernames and passwords) in order to log in to the service.

7 Administrative requirements

- i. When considering external cloud services, the agency chief executive should be satisfied that the administrative requirements listed below are met and will be adequately addressed within contractual arrangements with an external cloud services provider.

7.1 Agency access

7.1.1.1 Agencies must ensure NTG data and applications are available when required.

- i. The agency has surety that the external cloud services provider will:
 - a) allow access to the external cloud services for legitimate agency business by authorised users at all times required, with no unplanned downtimes
 - b) ensure no interruption to services required by the agency through having robust business continuity arrangements in place
 - c) prevent access to agency data by non-authorised persons and entities for the duration of the arrangements with the provider and beyond.

7.2 Data ownership

7.2.1.1 Agencies must ensure that ownership of government data is explicitly retained by the NTG in contracts with the cloud services provider.

7.3 Data sovereignty

7.3.1.1 Agencies must understand and ensure the sovereignty of NTG data held with an external cloud services provider is appropriate and acceptable.

- i. The physical location of agency data (including back-ups) is known and accepted, with data relocation by the cloud services provider requiring the agency's prior consent. The impact of applicable laws, including foreign laws, have been considered and there is certainty that agency obligations (including obligations under the privacy provisions of the *Information Act* (NT)) with respect to data storage locations will be met.
- ii. The contract with the external cloud services provider is to stipulate the data location, restrict data relocation without agency consent and align with NT legislative requirements.

7.4 Records management and Freedom of Information

7.4.1.1 Agencies must ensure that their obligations under the *Information Act* are able to be met.

- i. The agency must be confident that the contractual arrangement with the external cloud services provider will enable the agency to meet its Freedom of Information and records management obligations under the *Information Act* (NT); the **records management standards for public sector organisations in the Northern Territory**; and any other recording or reporting obligations that may be applicable, such as requirements specified in agreements with the Australian Government.

7.5 Audit

7.5.1.1 Agencies are subject to audit by the NT Auditor-General under the *Audit Act* (NT) and are required to provide authorised auditors with full access to agency records, systems and information.

- i. Agencies are to give consideration as to how audit requirements will be met for information held by an external cloud services provider on the agency's behalf, including audit access and review of processes.
- ii. Agencies are to incorporate appropriate audit provisions within their contractual arrangements with an external cloud services provider.

8 Procurement and contract management requirements

8.1 Procurement

8.1.1.1 Agencies must comply with the NTG Procurement Framework when buying external cloud services, including the principles of open tendering, fairness and equity; governments buy local policy and value for Territory.

- i. Sourcing an external cloud services provider is no different to sourcing supply of any other service. Agencies are required to follow normal processes and comply with the *Procurement Act* and directions.

8.2 Contracts

8.2.1.1 Agencies must ensure that contracts with external cloud services providers appropriately protect the NTG's interests and are in accordance with NTG contracting terms.

8.2.1.2 Agencies must ensure that suitable contractual agreements are in place prior to allowing NTG data or computing environments to be accessed by or provided to an external cloud service provider.

- i. Contractual arrangements will be agreed through the procurement process, based on standard NTG contract conditions, and supplemented by specific cloud appendices, incorporating ongoing contract management and contractor performance requirements.

8.2.1.3 Agencies must have practices in place to ensure that the contract is managed effectively throughout its term.

- i. Some elements of the procurement process and contract conditions are set out in this standard as they have particular relevance or importance for external cloud service arrangements. It is expected that existing NTG procurement and contract provisions will be generally sufficient for sourcing external cloud services, supplemented where necessary and outlined in this standard with specific provisions to protect the NTG.

8.3 Legal review and advice

8.3.1.1 Agencies must obtain and have regard to legal advice regarding legislative requirements, procurement and contractual arrangements.

- i. Controls throughout this standard make reference to agencies' rights, obligations, responsibilities and protections. Legal review and advice should be obtained where appropriate in relation to all such matters and in accord with normal government practices where agencies are considering new or changed business risks, undertaking procurement actions, initiating contractual arrangements or ensuring legislative compliance.
- ii. The legal advice should address any legal risks and mitigations, ways to protect the agency's rights and identification of any legal obligations the agency is required to meet.

8.4 Costs

8.4.1.1 Agencies must have certainty of the total costs of an external cloud services arrangement prior to entering into the arrangement.

- i. As part of the agency's due diligence evaluation, the agency should have knowledge of potential costs in the event the external cloud services provider fails to deliver the required services (costs to implement contingency plans).
- ii. All costs should be fully identified, including costs related to:
 - a) data transmission to and from the external cloud service
 - b) growth of data stored
 - c) audit and performance monitoring
 - d) transitioning-out at end of contract or on termination.

8.5 Liabilities and indemnities

8.5.1.1 Agencies must ensure contract agreements set out appropriate provisions for liabilities and indemnities, including adequate compensation in the event of data loss or misuse by the cloud services provider.

8.6 Contractor performance management

8.6.1.1 Agencies must ensure agreements with external cloud services providers incorporate adequate provision for contractor performance management over the contract term.

- i. Provisions for contractor performance management should include:
 - a) holding the provider to meaningful, measurable and auditable service levels, with consequences for non-delivery or not attaining required service levels
 - b) specifying response times the provider is required to meet

- c) assuring continuity and flexibility of service, with ability to quickly recover from any disaster events
- d) full reporting on contract performance by the service provider on a stipulated regular basis
- e) provision to independently audit the service provider's compliance with contract requirements and address penalties for any non-compliance.

8.7 Subcontractors

8.7.1.1 Agencies must understand arrangements and have visibility of any third parties utilised by the external cloud services provider in delivering their services.

- i. The requirements under this standard are to be applied equally to subcontractors and third parties of the external cloud services provider that are integral to delivering the cloud services to the agency.
- ii. The agency should obtain appropriate assurance regarding use of subcontractors by the service provider and apply strict controls within their contract with the external cloud services provider.

8.8 Termination rights and transition-out provisions

8.8.1.1 Agencies must ensure that the rights and obligations of the parties to a cloud services arrangement for disengagement or transition-out adequately protect the NTG's interests and are clearly prescribed.

- i. While much focus is placed on ensuring appropriate protections for the NTG in establishing an external cloud service arrangement, it is equally important that agency information can quickly, efficiently and accurately be extracted from the external cloud service provider's environment should this become necessary.
- ii. In the event that the arrangement with the external cloud services provider ceases, it is critical that agencies have rigorous provisions in place to ensure that:
 - a) NTG data is not left stranded in the provider's environment.
 - b) Full and complete data can be returned to the NTG or transferred to another external cloud services provider in a usable form.
 - c) The transfer can be achieved promptly to maintain seamless service delivery for agency clients.
 - d) The agency has certainty that the external cloud services provider has not retained copies of NTG data or in any way compromised the NTG data.
- iii. Contracts with external cloud services providers are to address the circumstances in which the agreement may be terminated, including:
 - a) termination for convenience and early termination fees: Where there is provision for early termination, agencies should consider payments applicable to the early termination. If compensation is appropriate, it should not exceed reasonable costs associated with the termination and would not, for example, extend to additional costs such as to cover loss of profit on the part of the provider

- b) termination for default of the service provider: the agency should ensure that it has the right to terminate for default where the provider does not meet the agency's reasonable requirements as set out in the agreement
- c) termination for likely or actual insolvency of the service provider: the agency should consider conditions of a quick disengagement if the service provider is facing bankruptcy
- d) circumstances in which the service provider has a right to terminate: the agency should consider including a sufficiently long notice period before the termination becomes effective to enable the agency to find a suitable alternative provider.

8.8.1.2 Agencies must ensure that, on termination or transition-out of an external cloud services arrangement, all agency data will be readily and reliably recoverable.

- i. The recovery and transmission of data in the event of a change in arrangements with the external cloud services provider must be accommodated in contractual arrangements. It is possible to not be able to retrieve data under circumstances where arrangements end abruptly and involve third parties.

8.9 Change of control

8.9.1.1 Agencies must ensure all rights survive substantive changes in circumstances

- i. The contractual arrangements with an external cloud services provider must include certainty as to the respective rights and obligations of the parties in the event that:
 - a) a change in control or ownership of the external cloud services provider occurs
 - b) administrative arrangements change within the NTG that changes the agency.
- ii. In line with standard contract provisions, the rights and obligations of the parties need to survive the above changes but allow the NTG the opportunity to reconsider its requirements and continuation of the contract if the change in the external cloud services provider introduces new or greater risks or is incompatible with the NTG position or direction.
- iii. A change in control or ownership of an external cloud services provider should trigger a further due diligence evaluation by the agency, including an updated risk assessment and NTG ICT Security assessment in accordance with this standard.

8.10 Periodic review

8.10.1.1 Agencies must periodically review arrangements with external cloud services providers to ensure that the contract reflects the service being provided.

8.10.1.2 At a minimum, agencies must undertake a detailed risk assessment prior to renewal or extension of arrangements with an external cloud services provider.

9 Other requirements

9.1 Key stakeholder acceptance

9.1.1.1 Agencies must take care to reduce any exposure for the NTG or opportunity for future complaints or disputes relating to the manner in which the data is managed and protected.

- i. The agency has a responsibility to ensure that other key parties involved in creating, receiving, handling or dealing with data to be stored by the external cloud service know and understand the service and data storage arrangements.
- ii. Where the parties would reasonably have an expectation that their data is retained by the agency, it is appropriate for the agency to inform them, assure them if required and address issues that may arise.

9.2 Community

- i. It is incumbent on the agency to consider the needs and expectations of the community in delivering services and managing data, particularly if the data constitutes personal information relating to Northern Territory citizens or commercial data. Some circumstances are specified in the *Information Act*, where the prior consent of the individuals to whom personal information relates is required before actions can be taken with the data. The agency would need certainty of its position regarding provision of such data to an external cloud services provider or appropriate permissions or protections.
- ii. The agency should consider communications and consultation to provide appropriate comfort to the community and the agency's clients regarding data management through an arrangement with an external cloud services provider.
- iii. Agency consideration of any potential reputation risk for the NTG and effective mitigation actions are recommended.

10 External cloud services register

10.1 Maintain register

10.1.1.1 Agencies must maintain a register of external cloud services utilised.

- i. The register must include, at a minimum, details of the:
 - a) external cloud service provider (e.g. name, location etc.)
 - b) nature of the arrangement (e.g. type of cloud service, matters particular to the arrangement)
 - c) nature of the information stored by the external cloud service and the security classification level of such information
 - d) physical location of the data centre(s) at which the agency's information is stored
 - e) copy or link to the risk assessment of the external cloud service required by this standard
 - f) certification by the agency chief executive (copy of the signed certification)

- g) term of the contractual arrangement with the external cloud service provider (including commencement and expiry dates and rights of renewal, if any)
 - h) costs of the arrangement
 - i) reference to the contract agreement with the service provider.
- ii. Given the passing of control that occurs with an external cloud services provider and the risks this introduces for the NTG, an agency register of external cloud service arrangements is a necessary governance measure.

10.2 Allocate responsibility

10.2.1.1 Agencies must assign a position or staff member with responsibility to manage the relationship with each external cloud service provider.

- i. It is recommended that this be the chief information officer of the agency or an equivalent senior position.

11 Glossary of acronyms

Acronym	Full form
ASD	Australian Signals Directorate
CCSL	Certified cloud services list (provided by ASD)
ICT	Information and communications technology
IPPs	Information privacy principles as prescribed in schedule 2 of the <i>Information Act</i>
NTG	Northern Territory Government
IRAP	Information security registered assessors program

12 Supporting references

12.1 NTG documents

- Cloud computing policy
- Records management standards for public sector organisations in the Northern Territory
- Treasurer's directions ICT series

12.2 Australian Government documents

- Australian Government Protective Security Policy Framework ²()
- Australian Government Information Security Manual – Controls – Outsourced General Information Technology Services, Outsourced Cloud Services sections ³

² <https://www.protectivesecurity.gov.au/Pages/default.aspx>

³ http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf

- Australian Government Information Management Office, Negotiating the cloud – legal issues in cloud computing agreements – Better Practice Guide⁴

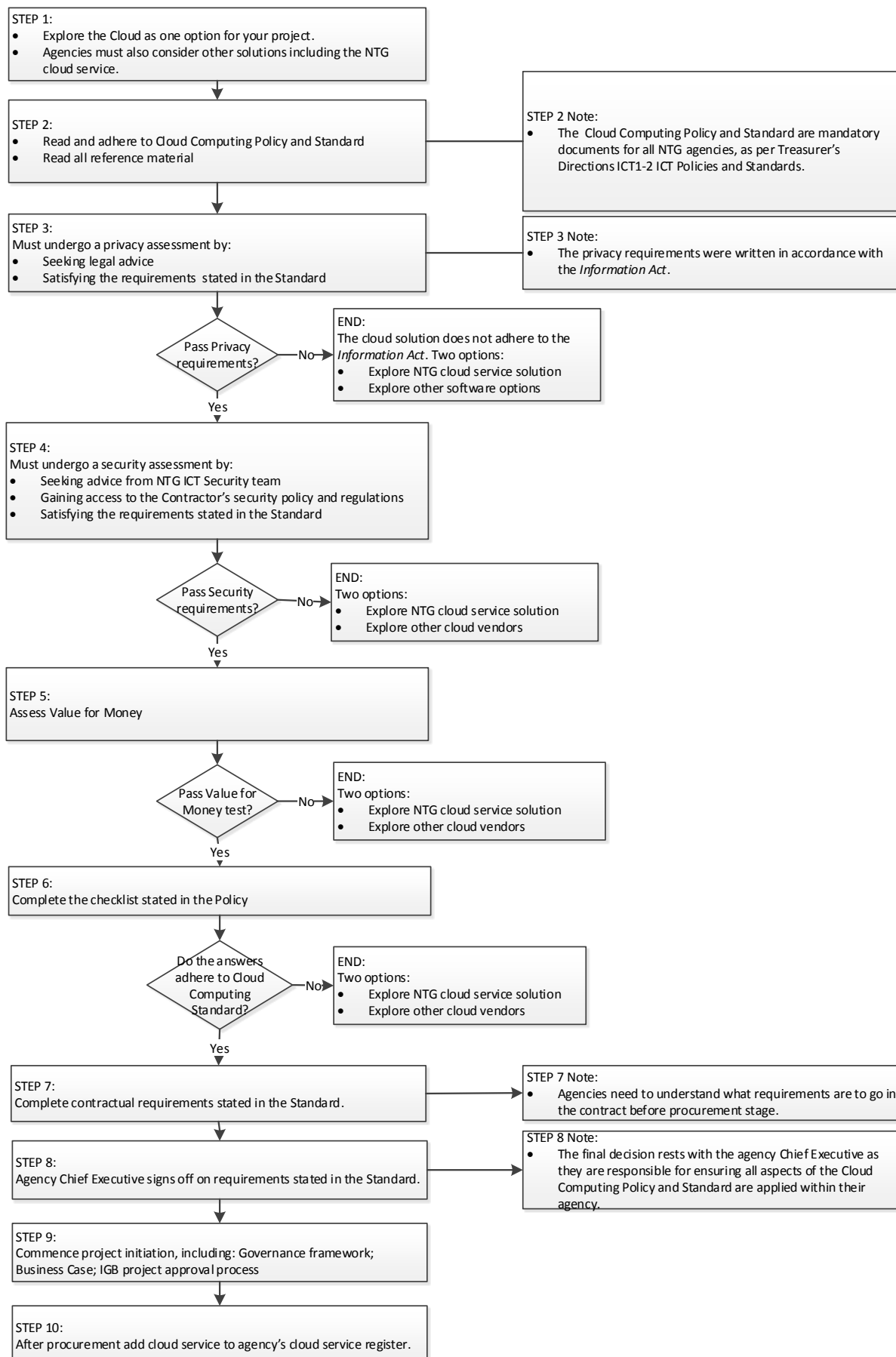
⁴ <http://www.finance.gov.au/cloud/>)

Appendix A: External cloud service proposal

Chief executive checklist	
Agency	
Service proposed	
Entering the agreement	
Agreement in writing	<input type="checkbox"/>
Legal advice obtained	<input type="checkbox"/>
Protection of information	
Privacy	<input type="checkbox"/>
Data ownership	<input type="checkbox"/>
Data sovereignty (application of foreign laws/transborder data transfer)	<input type="checkbox"/>
Data security	<input type="checkbox"/>
Confidentiality	<input type="checkbox"/>
Records management and freedom of information requirements	<input type="checkbox"/>
Access	<input type="checkbox"/>
Audit	<input type="checkbox"/>
Liabilities and indemnities, including compensation for data loss and/or misuse	<input type="checkbox"/>
Subcontractors	<input type="checkbox"/>
Performance management	
Service levels	<input type="checkbox"/>
Response times	<input type="checkbox"/>
Flexibility of service	<input type="checkbox"/>
Business continuity and disaster recovery	<input type="checkbox"/>
Ending the agreement	
Termination rights	<input type="checkbox"/>
Disengagement/transition-out procedures	<input type="checkbox"/>
Other legal issues	
Dispute resolution/choice of law	<input type="checkbox"/>
Costs detailed	<input type="checkbox"/>
Change of control	<input type="checkbox"/>
Unilateral change of contract terms	<input type="checkbox"/>
Third parties	
Acceptance by key stakeholders	<input type="checkbox"/>
Community comfort/reputational risk	<input type="checkbox"/>

Appendix B: Flowchart

Cloud Computing Flowchart (pre Approval / Procurement)



Appendix C: Flowchart (as text)

Step 1

- Consider the re-use or sharing of an existing solution, including the NTG cloud service.
- Explore the external cloud as one option for your project if no existing or internal solution is acceptable.

Step 2

- Read and adhere to the **Cloud computing policy and standard**.
- Read all reference material.

Notes:

- The **Cloud computing policy and standard** are mandatory documents for all NTG agencies, as per Treasurer's directions ICT1-2 ICT policies and standards.

Step 3

Must undergo a privacy assessment by:

- seeking legal advice
- satisfying the requirements stated in the standard.

Notes: The privacy test was written in accordance with the *Information Act*.

Question: Pass privacy requirements?

- If answer is no: End of flowchart – The cloud solution does not adhere to the *Information Act*.
Two options:
 - explore NTG cloud service solution
 - explore other software options.
- If answer is yes: Continue to step 4.

Step 4

Must undergo a security assessment by:

- seeking advice from NTG Security team (ictsecurity.ntg@nt.gov.au)
- gaining access to the contractor's security policy and regulations
- satisfying the requirements stated in the standard.

Question: Pass security requirements?

- If answer is **no**: End of flowchart. Two options:
 - explore NTG cloud service solution
 - explore other software options.
- If answer is **yes**: Continue to step 5.

Step 5

Assess value for money.

Question: Pass value for money test?

- If answer is **no**: End of flowchart. Two options:
 - explore NTG cloud service solution or
 - explore other software options.
- If answer is **yes**: Continue to step 6.

Step 6

Implement risk mitigation strategies.

Question: Can the risks be adequately mitigated?

- If answer is **no**: End of flowchart. Two options:
 - explore NTG cloud service solution or
 - explore other software options.
- If answer is **yes**: Continue to step 7.

Step 7

Complete contractual requirements stated in the standard.

Note: All NTG data stored in the cloud must be accessible to the right people and secure during the contract and when the contract has completed

Step 8

Agency chief executive signs off on requirements stated in the standard.

Note: The final discussion rests with the agency chief executive as they are responsible for ensuring all aspects of the **Cloud computing policy** and **standard** are applied within their agency. The chief executive checklist in Appendix A can be used to assist in ensuring all aspects have been covered.

Step 9

Commence project initiation, including:

- Governance framework
- Business case
- IGB project approval process.

Step 10

After procurement add cloud service to agency's cloud service register.

13 Document control

Document details	
Responsible agency	Department of Corporate and Information Services (DCIS)
Contact details	Digital Policy Unit, Office of Digital Government, Digital.Policy@nt.gov.au
Date and version	18 September 2017 Version 2.1
Approved by	Minister for DCIS, Hon Lauren Moss
Date approved	17 July 2017

Change history			
Version	Date	Author	Change details
2.0	July 2017	DCIS	Major review. Approved and published.
2.1	September 2017	DCIS	Internet version: excludes reference to internal documents.