

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.**

17 September 2017
Version 2.1

Contents

1	Policy statement.....	3
2	Purpose.....	3
3	Cloud computing defined	3
4	Scope	3
5	Responsibilities.....	4
6	Controls	4
7	Glossary of acronyms.....	5
8	Supporting references	5
	8.1 Australian Government security documents.....	5
9	Document control.....	6

Authority

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 policy specifies the accountability requirements and controls to enable effective use of cloud computing. Cloud computing services are generally externally based and cover a spectrum of ICT related services from infrastructure through to software.

The use of cloud computing by agencies can deliver benefits in terms of increased productivity, better services to the public and reduced costs through leveraging economies of scale.

Transition to external cloud services reduces agency control over service delivery and NTG data, and introduces a range of new or additional risks, including security, legal, financial, commercial, business continuity and government reputational risks that need to be addressed.

A careful and complete evaluation of computing, security and business requirements is essential prior to selecting a computing service solution.

This policy is to be read in conjunction with the supporting **cloud computing standard** which sets out the minimum requirements for agency evaluation of computing service solutions.

3 Cloud computing defined

- i. 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,¹ which may be viewed in full at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.
- ii. 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.

4 Scope

- i. The scope for this policy covers all NTG agencies and GOCs.
- ii. This policy applies to NTG agency staff or service providers responsible for procuring and/or managing the use of external cloud computing services by the agency.
- iii. This policy and its supporting standard cover the mandatory requirements for agencies in selecting and using cloud computing services.

¹ US Department of Chamber and Commerce, National Institute of Standards and Technology (NIST), definition of cloud computing, special publication 800-145 September 2011.

5 Responsibilities

- i. Agency chief executives are responsible for ensuring this policy is applied within their agency and adequate resources are allocated to policy implementation.
- ii. Agency chief executives are responsible for ensuring that the **cloud computing policy** and Standard requirements are satisfied before approving an external cloud service.
- iii. Agency chief information officers/ICT directors are responsible for completing the requirements set out in this policy and the **cloud computing standard**, including risk assessment, risk mitigations, value/benefit analysis and seeking agency chief executive certification prior to procuring an external cloud service for the agency, regardless of value.
- iv. In instances when more than one agency is involved, the lead agency chief executive will be responsible, unless otherwise stated in the contractual agreement. Where adjunct agencies have specific privacy or legal requirements the respective agency chief executive will be responsible for such additional requirements.

6 Controls

- i. Agencies must adhere to the mandatory requirements detailed in this policy and its supporting standard.
- ii. Agencies are to undertake due diligence investigations necessary to enable the agency chief executive to make fully informed decisions about computing solutions that will deliver the best outcome for government and withstand independent scrutiny.
- iii. Agencies due diligence processes are to commensurate with the scale, sensitivity, confidentiality and complexity of the service and data involved. Thorough evaluation of external cloud computing services will be required as the security posture of external services is not known to the NTG. 'External cloud service' is defined in the standard and includes externally hosted NTG websites.
- iv. NTG cloud services should be assessed as for other computing services. The security posture of the NTG cloud service is known which will streamline assessment. The NTG cloud service undergoes regular independent audits and complies with NTG ICT policies and standards and therefore satisfies NTG cyber security requirements.
- v. Where more than one agency is involved, the lead agency must consider and address the adjunct agencies' requirements in the planning and set-up of cloud computing services.
- vi. Agencies must comply with the *Information Act* and establish appropriate security and internal process controls, having regard to the nature of the cloud service and the type of information to be hosted in the cloud.
- vii. Controls are set out more fully in the cloud computing standard which covers the following:
 - a. The responsibility of the agency chief executive to make an informed decision in considering adoption of an external cloud service, including specific criteria which must be reviewed and certified by the chief executive before an external cloud service is procured
 - b. Privacy requirements – overview of the privacy requirements under the *Information Act*
 - c. Security requirements – including key requirement to consult NTG ICT Security before procuring an external cloud service and specific security measures which must be implemented.

- d. Other requirements – includes requirements that the agency chief executive will acknowledge before certifying.
- e. Reuse requirement – consider the re-use of existing services, both NTG hosted services and existing cloud services, before procuring a new solution.
- f. Contractual arrangements – requirements for documenting the arrangement between the agency and the external cloud service provider.
- g. External cloud services register – requirement for a register of external cloud service providers to be maintained, regardless of value.
- h. Supporting resources – a checklist for use by the agency chief executive, to ensure key requirements have been met and a flowchart to assist agencies in understanding the steps that must be followed in order to procure an external cloud service.

7 Glossary of acronyms

Acronym	Full form
ICT	Information and Communications Technology
NTG	Northern Territory Government

8 Supporting references

- i. Cloud computing standard.
- ii. Treasurer's directions ICT series.

8.1 Australian Government security documents

- i. The NTG takes close regard of the Australian Government security documents and seeks to adopt and adapt control measures and mitigation actions wherever feasible. The key Australian Government documents are:
 - a. Australian Government protective security policy framework
 - b. Australian Government information security manual.

9 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.