# Cloud computing policy

**Policy overview**

The following table summarises key information regarding this Ministry-wide internal policy.

<table>
<thead>
<tr>
<th>Name of policy</th>
<th>Cloud computing policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>This policy outlines the assessment criteria to be applied before selecting a third-party provider, the requirements to be included in the contract and the procedures to be followed to ensure compliance with standards, guidelines and architectures.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>This policy applies to all Ministry staff who procure or commission internal and sector-facing services that propose to use outsourced or cloud service provider services.</td>
</tr>
<tr>
<td><strong>Definitions</strong></td>
<td>Below are a list of common terms used in this policy document.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Word or phrase</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud service provider</td>
<td>A company that offers some component of cloud computing - typically ‘Infrastructure as a Service’, ‘Software as a Service’ or ‘Platform as a Service’ - to other businesses or individuals.</td>
</tr>
<tr>
<td>‘Infrastructure as a Service’</td>
<td>An all-of-government agreement that offers a catalogue of IT components including: data centre facilities, computing, storage and backup services.</td>
</tr>
<tr>
<td>‘Telecommunication as a Service’</td>
<td>An all-of-government agreement that delivers a catalogue of cross-government telecommunications and security services.</td>
</tr>
</tbody>
</table>

**Owner**

Chief Technology & Digital Services Officer, Ann-Marie Cavanagh

**General enquiries**

Principal Advisor, Standards

**Review date**

Annually - to ensure the policy stays current due to changing technology requirements.
Cloud computing policy

Introduction

The Ministry needs to meet its responsibilities by ensuring the security, privacy and ownership rights of information held with outsourced or cloud service providers is appropriate, clearly specified and built into the contractual arrangements for that service.

Key considerations for cloud computing are:

- business risk
- information security
- information management
- privacy
- business continuity
- disaster recovery
- legislative obligations
- service level and key performance indicators
- commercial constructs
- IS architectural fit.

Policy

Cloud computing solutions will be considered alongside traditional in-house solutions as an appropriate response to business needs. In compliance with the Cabinet’s directive (Cloud First) - where a cloud-based solution meets business needs, it will be preferred to a traditional in-house solution.

Regardless of the cloud computing solution chosen, the Ministry must be able to demonstrate compliance with all relevant legislation such as:

- the Privacy Act 1993
- the Public Records Act 2005

As part of the process of evaluating a cloud computing solution, the following principles must be applied:

- Cloud computing solutions, usually offered by a cloud service provider, will be evaluated on a case-by-case basis against the Ministry’s policies, principles and guidelines, and Ministry/sector standards.
- Government Chief Information Officer and Privacy Commission guidelines and requirements should be followed as part of the assessment of a solution.

• Cloud computing solutions must deliver the same or better levels of service as an in-house solution to ensure business continuity, in line with the requirements of the business service being delivered.

• Cloud computing solutions must safeguard the security and privacy of the Ministry’s data, and comply with all appropriate security and privacy requirements.

• Impacts on the operational stability or performance of the Ministry’s core systems need to be considered when choosing a cloud computing solution.

• Only data classified as RESTRICTED or below may be stored in a cloud computing solution/service.

• Cloud computing solutions will be delivered using the same processes and controls as any other technology solution at the Ministry.

Guidance

This section provides further information on interpreting the policy and provides guidance to support your decision-making process.

For a summary of what cloud computing is, the models available and how cloud computing is typically implemented, refer to the paper by the National Institute of Science and Technology in the US in the ‘Related reading’ section. Understanding this information is helpful when assessing cloud computing solutions in the context of the Government Chief Information Officer’s cloud risk assessment.

Any questions or concerns relating to assessing the applicability of a cloud computing solution should be raised with Technology & Digital Services (T&DS).

General:

• Check whether the cloud service being considered has already been accepted by the Government Chief Information Officer to prevent potential duplication of effort or unnecessary cost/effort.

• All-of-government ‘Infrastructure as a Service’ services have already been accredited by the Government Chief Information Officer who recommends each agency performs the cloud risk assessment to understand the relevant requirements. For the Ministry, cloud risk assessments must be completed for ALL projects that may use one or more cloud computing services.

• Hosting cloud solutions, that will store personally-identifiable data (patient or staff information), in a public cloud facility in Australasia is preferable to hosting outside of the region.

• If data stored with a cloud service provider is to be encrypted this should be done using cryptographic keys owned and managed by the Ministry’s T&DS group (please discuss with a staff member in the T&DS team).

• The Government Chief Information Officer considers mobile apps to be cloud services if “they store, process or transport agency information outside your network boundary”.

3
In all cases, a cloud computing solution will only be considered after a thorough risk evaluation has been completed, reviewed and accepted by the Ministry’s Chief Information Security Officer or delegate.

Cloud computing solutions must be supported by facilities that meet Uptime Institute Tier-3 or higher rating. Anything less than this needs extra resiliency capabilities created by the project team.

Security:
- Guidance and directives in the Health Information Security Framework (HISO 10029:2015) and NZ Information Security Manual must be adhered to when designing or evaluating a cloud-based solution.
- Check the advice and accreditations on the government’s ict.govt.nz website.
- All personally identifiable information must be classified as ‘In Confidence’ (prefixed with either ‘Medical’, ‘Commercial’ or ‘Staff’) as the minimum security classification.

Connectivity & integration:
- Consider what data or applications you want/need to connect with and incorporate these into your review from the beginning.
- Integrating the vendor’s cloud solution with other services/data sets/solutions should follow the HISO approved/endorsed interoperability standards (HISO 10013:2015, HISO 10040.0:2012).
- If the cloud vendor does not support these HISO standards, please discuss with the Ministry’s enterprise architects in T&DS.
- Connectivity to all services outside of the Ministry network (including for the purposes of system-to-system integration) must be secured using a Ministry-approved solution. Cloud service providers must support this capability.

Sourcing:
- ‘Consuming Infrastructure as a Service’ from Amazon Web Services or Microsoft Azure via the all-of-government ‘Infrastructure as a Service’ providers is already covered under the contract those providers have with the Department of Internal Affairs (DIA).
- Purchasing cloud services not covered by the all-of-government agreements are subject to the government’s rules of Sourcing. Review the guidance provided by the DIA on this website and the government’s procurement website.
- The Ministry’s non-functional requirements must be incorporated in all procurement activity, including for cloud-based services.
- Contracting with cloud-solution providers, not covered by an all-of-government agreement, is similar to contracting with other outsourcing vendors. Similar rigour and data governance considerations should be included in all contracts with cloud service providers. Things to incorporate (this is not an exhaustive list, regularly check the ict.govt.nz website for additional advice):
• a Non-Disclosure Agreement (recommended before provisioning any service)
• data ownership (the Ministry retains exclusive ownership of ALL data held in a cloud provider’s solution which was entered by Ministry staff, systems or affiliates in all media forms e.g. online, backup and archive etc)
• any other standard intellectual property clauses (as are relevant to the service)
• data location (the countries where Ministry data can be held should be explicitly stated in contracts – this should be based on the outcome of the cloud risk assessment and any associated privacy impact assessment)
• privacy legislation compliance
• Service Level Agreements (to meet availability, performance, and recovery requirements)
• service management processes
• the application of appropriate retention policies to stored data based on its classification (see ‘Data governance’ below) - this means the cloud service provider’s solution must not hinder compliance with the Public Records Act
• a clear process documenting the responsibilities of each party with respect to extracting Ministry data and destroying data at the end of the contract
• provision for a cloud service provider being taken over/bought-out by another organisation (this should include ensuring the ownership, access rights and protection of any data the Ministry owns cannot be lost when there is a change of cloud service provider ownership)

- copies of potential cloud service providers’ most recent standards-based security assessment/assurance as early in the procurement cycle as possible e.g. SOC2 Type 2 (operational effectiveness) audit report etc.
- completion of a section of the Government Chief Information Officer’s cloud security risk assessment by cloud solution vendors (ensure plenty of time has been left for the cloud service provider to do this, as accreditation for use of their services cannot be obtained without that section being completed).

**Data governance:**

- All personally-identifiable information **must be** encrypted at rest and in transit (see the requirement regarding encryption in ‘General’ above) when stored in a data centre outside of an ‘all-of-government ‘Infrastructure as a Service’ offering. This includes transactional, backup and archival data on all electronic media types.
- The cloud service provider **should** provide an easy mechanism to report on all people who have information stored in its solution/service.
- All data to be stored in a cloud service must be classified and appropriate retention period controls implemented. See the Archives NZ [website](#) for the most current retention rules relating to New Zealand health data.
Processes and/or procedures

This policy applies to all Ministry staff involved in:
- procuring new IT based solutions that could be hosted outside of the Ministry’s core IT systems
- migrating existing IT systems to an outsourced or cloud service provider
- hosting newly developed IT sector solutions.

Related reading

This information will assist the Senior Business Advisor, Office of the Deputy Director-General, Corporate Services when preparing the content of this document for MoHAWK.

Other relevant Ministry policies:
- Information Security Policy
- Data Classification Policy
- Procurement Policy
- Financial Delegation Policy.

Example of how scope and responsibility change by type of cloud service:

<table>
<thead>
<tr>
<th>Area of responsibility</th>
<th>Type of Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IaaS</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Software, user applications</td>
<td></td>
</tr>
<tr>
<td>Operating systems, databases etc</td>
<td></td>
</tr>
<tr>
<td>Virtual infrastructure (hypervisor, virtual appliance, VMs, virtual networks etc)</td>
<td></td>
</tr>
<tr>
<td>Computer and network hardware (processors, memory, storage, cabling etc)</td>
<td></td>
</tr>
<tr>
<td>Data Centre (physical facility)</td>
<td></td>
</tr>
</tbody>
</table>

Cloud customer responsibility

Cloud Service Provider responsibility

The following paper from the National Institute of Science and Technology in the US provides an excellent overview of cloud computing including a definition, essential characteristics and typical deployment models: