Cloud Computing Policy

Audience and scope:

This policy is relevant to all staff, students and other users of computer systems owned or managed by MIT and EnterpriseMIT.

Document management and control

Policy Number	ICT2	**Consultation Scope**	Senior Leaders, Leadership Team
Category	Management	**Approval Bodies**	Chief Executive
Policy Owner	CFO and Director Corporate Services	**Review Dates**	January 2017
Policy Contact Person	Head of Technology Service		

Amendment history

Version	Effective Date	Created/Reviewed by	Reason for review/Comment
.001	30 November 2015	Melanie Visser	Created new policy.
.002	4 February 2016	Melanie Visser	Updated document with feedback from Technology Services Management Team, Legal, People & Culture.

Table of Contents

Cloud Computing Policy

Purpose

The purpose of the Cloud Computing Policy is to ensure that the confidentiality, integrity and availability of MIT's information is maintained when services are delivered through a cloud computing environment. As the cloud can be private or public, local or international it is important to ensure that arrangements are supported by a service agreement, meet MIT's requirements for information security and enable statutory and legislative obligations to be met.

Background

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

In August 2012, Government released [CAB Min[12] 29/8A][2] directing a "cloud first" policy for the State Sector. The rationale was to allow agencies "to consume ICT as a service which leads to smarter investment and savings across the public sector."

The benefits[3] that Government saw from cloud computing were:

- Cloud computing solutions are scalable: agencies can purchase as much or as little resource as they need at any particular time. They pay for what they use.
- Agencies do not have to make large capital outlays on computing hardware, or pay for the upkeep of that hardware.
- Cloud computing provides economies of scale through all-of-government volume discounts. This is particularly beneficial for smaller ICT users.
- Agencies can easily access the latest versions of common software, which deliver improved and robust functionality, and eliminating significant costs associated with version upgrades.
- If agencies are able to access the same programmes, and up-to-date versions of those programmes, this will improve resiliency and reduce productivity losses caused when applications are incompatible across agencies.

The Government recognised that while cloud computing offered significant financial and operational benefits, there were associated risks that must be managed. To this end the Government released its Cloud Computing Risk and Assurance Framework, [CAB Min[13] 37/6B][4] in October 2013 which all State Service agencies are expected to follow. To support this

[1] http://www.nist.gov/itl/cloud/index.cfm
[2] http://ict.govt.nz/assets/Uploads/Documents/CabMin12-cloud-computing.pdf
[3] https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/
[4] https://www.ict.govt.nz/assets/Cabinet-Papers/Cab-Minute-Cloud-Computing-Risk-and-Assurance-Framework-Oct-2013.pdf

the Government CIO produced the "Cloud Computing: Information Security and Privacy Considerations"[5] publication, which needs to be followed to ensure adherence to the framework.

Policy

MIT will follow the intent of Government and move to fully utilising cloud computing in order to accrue the advantages that have been identified. MIT will comply with Government's Cloud Computing Risk and Assurance Framework for all Cloud Computing initiatives.

MIT will implement the following controls for Cloud services:

1. Information Security Requirements

1.2 MIT must confirm the responsibilities of the cloud service provider with regard to information security. These responsibilities must be documented in an agreement which is signed by both MIT and the cloud service provider and approved in accordance with the Agreement Approval Policy.

1.3 The cloud service provider must sign a confidentiality agreement as part of their contract. This may include:

- Definition of the information to be protected.
- Duration of the agreement.
- Termination procedure.
- Security responsibilities to avoid information disclosure.
- Notification process for reporting any breaches of confidentiality.
- Non-compliance actions.
- Ownership of the information.
- Permitted use of the information or system by the service provider.
- Right to monitor and audit.

2. Authorisation

2.1 It is not appropriate for users to sign up to cloud computing services without MIT undertaking a full assessment of the value of the service and the potential risks involved. As cloud computing services may include the external hosting of data, applications and the use of hardware supplied by a third party, MIT must be confident that the benefits of subscribing to the service outweigh the risks and the service, and that MIT's information will be available as required and sufficiently protected from vulnerabilities and threats. For this reason, no cloud based system will be implemented unless it has been evaluated by Technology Services and deemed to comply with the Government's Cloud Computing Risk and Assurance Framework.

[5] http://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf

3. Risk Assessment

3.1 MIT should identify the risks to information and information processing facilities caused by the use of cloud computing services and implement the appropriate security controls and agreements before starting to use the service. The security requirements related to customers accessing organisational assets should be addressed using customer agreements which contain all identified risks and security requirements.

The identification of risks specific to cloud computing services should take into account that:

- The information is stored in the hardware owned by cloud service provider.
- Cloud service provider may use other cloud computing services.
- Business processes of other cloud service users may share the same hardware.
- After the termination of use of the cloud computing services, the system resource used by the services is generally being reused.
- Some of MIT's information security requirements and controls may be ineffective upon use of cloud computing services.
- Changes within the operating environment (e.g. mobility). that can be achieved by using cloud computing services. Business operation, e.g. mobile computing, may change through the use of cloud computing services.

3.2 MIT must evaluate the use of cloud computing services with regard to the risks associated with business continuity including:

- Failure of cloud computing service.
- Internet connectivity.
- Service unavailability by law enforcers' confiscation.
- Termination of cloud computing service.
- Potential vendor lock-in.

4 System Requirements

4.1 The Head of Technology Services must ensure that cloud computing services have the capacity and functionality to deliver the expected level of system performance.

4.2 MIT must define which mobile devices and methods of connectivity are approved for the cloud computing environment. Security controls must be applied based on the functionality of the mobile device and service used.

5. Protecting Systems from Risk

5.1 MIT must ensure that the cloud service provider has implemented sufficient measures to combat the introduction of malicious code. MIT must also implement measures internally to protect information systems from any threat originating from this source.

5.2 The Head of Technology Services must approve the networks that may be used for cloud computing services. If a public network is approved additional technical and security controls may be required to ensure the information remains secure.

5.3 As cloud service providers often use shared infrastructure and network services (like active directory), MIT must ensure that this is an appropriate platform for the information involved and that there is adequate security to protect it from unauthorised access.

Where information is confidential or sensitive, system segregation or complete isolation may be a requirement and if this is the case these requirements must be included in contractual agreements.

6. Monitoring, Logging and Audit

6.1 MIT should regularly monitor and review the services, reports and records provided by the cloud service provider and must conduct a regular audit of the cloud service provider's performance in accordance with the service agreement. Faults within the system must be logged and reported.

6.2 Cloud computing services should be monitored to ensure that users are only performing activities that they have been authorised to perform. System administration functions carried out by the cloud service provider must also be logged. All logs must be protected from unauthorised access and modification so that evidence is not compromised if required for any purpose.

6.3 As part of any service contract, MIT must define its requirements with regard to the collection and retention of audit logs. The information recorded in the logs must be made available upon request and particularly when required for evidential purposes.

These requirements should determine the:

- Events to be logged.
- Information and data format to be recorded as audit logs.
- Retention period of audit logs.
- Interactively accessible period.
- Method of verifying integrity of audit logs.

6.4 MIT must include a regular audit of the cloud computing environment as part of the service agreement. The scope of the audit must be agreed by the cloud service provider and may include hardware, operating systems, applications, information and communications links.

7. Systems Management

7.1 The use of system utilities that have the potential to override system and application controls within the cloud computing environment must be strictly managed.

7.2 MIT must manage all changes made by the cloud service provider to systems and services that affect the security of information or systems within MIT's change management process. Testing and validating changes must form part of this process to ensure that systems are not adversely affected by any change made.

8. Management of Users

8.1 There must be formal registration and de-registration procedures in place for cloud computing users. As the management of this function may be external to MIT, the cloud service provider must ensure that an appropriate and agreed procedure for granting and

revoking access to systems is included in the service agreement.

8.2 MIT must ensure that systems and services provided by a cloud service provider include an appropriate and agreed secure method of authenticating users.

Where MIT has existing security requirements with regard to unique user IDs, password criteria and any requirement to use two factor authentication, biometrics or equipment identification, these must be applied in the cloud computing environment.

8.3 Users of cloud computing services must be restricted only to systems, applications and information they are authorised to access and use.

8.4 All users must be required to undergo the necessary training prior to working on the cloud based system. Training should be part of the transition plan for any new system.

8.5 Inactive sessions must be automatically shut down after a defined period of inactivity and for high risk applications the connection time is limited to specific hours of use.

9. Information Management

9.2 MIT must ensure that the cloud service provider has a backup and restore facility included within the service. This service must be appropriate to the classification of the system and information stored within it. The backup and restore facility must conform to MIT's backup requirements.

MIT must ensure that a copy of the backup is retrieved on a regular basis and that it is in a format that can be accessed if required.

9.3 Intellectual Property Rights and ownership relating to information, applications and systems must be specified in the cloud service agreement with the cloud service provider where appropriate. Any agreement relating to MIT's intellectual property must comply with the Intellectual Property Policy.

9.4 MIT must confirm that cloud service provider can retain business records on cloud computing service for the period required to comply with MIT's Records Management Policy and to meet any other financial, legal and statutory requirements.

9.5 Data protection and privacy must be ensured as required by MIT's Privacy Policy, relevant legislation, regulations, Government's Cloud Computing Risk and Assurance Framework and, if applicable, contractual clauses.

10. Business Continuity and Incident Management

10.1 Business Continuity/DR plans and procedures should include cloud computing services where this is used and to support business activities. All plans should be tested annually and involve the cloud service provider.

10.2 The Technology Services Service Desk is the formal channel for users to report processing problems,
access problems or security issues relating to the cloud computing service. Issues should be reported immediately to the cloud service provider. All security issues must be reviewed and reported to the Leadership Team annually. Examples include (but not limited to):

- Loss of service, equipment and facilities.

- System malfunctions or denial of service.
- Human error.
- Non-compliance with standards or guidelines.
- Breaches of physical security arrangements.
- Uncontrolled system changes.
- Malfunctions of software or hardware.
- Unauthorised access.

10.3 MIT must ensure that the cloud service provider has procedures in place for managing a security incident to ensure that systems are returned to a former trusted state. This process must include a process for two way communication and keeping MIT informed of progress, likely outcomes, ramifications and damage control.

10.4 In the event legal action relating to the use or management of the cloud computing service is warranted, evidence must be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Service agreements with the cloud service provider must determine the jurisdiction of the agreement as this determines which country's laws are applicable. Where possible, New Zealand law should be the governing law and exclusive jurisdiction for all agreements into which MIT enters.

Procedures

Please refer to the policy section.

Evaluation/Outcomes

Audit: The Risk and Assurance Manager may audit compliance with this policy as part of internal audit work programmes.

Compliance: The Head of Technology Services will monitor compliance.

Additional Information

Glossary

Term	Definition
Cloud computing	Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Intellectual property rights	'Intellectual property' means proprietary rights concerning all original work governed by the Copyright Act 1994, the Patents Act 1953, the Designs Act 1953, the Trade Marks Act 2002, the Layout Designs Act 1994, the Plant Varieties Act 1987 any amendments to these or subsequent acts and any other intellectual property law. It includes, but is not limited to: • Courses materials. • Research data and outputs. • Assessment materials. • Administrative materials. • Computer software, videos and recordings. • Creative, literary works, artwork. • Discoveries/innovations/inventions. • Patents, Copyright, designs, trademarks. • Patentable and potentially patentable subject matter and associated know how. • Plant variety. • MIT data.

Exemptions and dispensations

Any dispensations from the requirements of this policy, including any one-off circumstances, must be approved in writing by the CFO and Director Corporate Services.

Delegations

- Council Register of Permanent Delegations and Authorisations.
- Statute 2: The Delegations and Authorisations Statute.

- Delegated Authorities Policy (FIN2).

Relevant Legislation

- Copyright Act 1994.
- Privacy Act 1993.
- Unsolicited Electronic Messages Act 007.
- Education Act 1989.
- Fair Trading Act 1986.
- Harmful Digital Communications Act 2015.
- Human Rights Act 1993.
- Films, Videos and Publications Classification Act 1993.

Legal Compliance

This policy complies with MIT's statutes, regulations and relevant legislation.

Associated documents

The following documents are associated with this policy:

- Intellectual Property Policy (AM10).
- Delegated Authorities Policy (FIN2).
- Procurement Policy (FIN3).
- Agreement Approval Policy (LC1).
- Fraud Prevention and Response Policy (LC2).
- Records Management Policy (LC4).
- Information Act Requests Policy (LC5).
- Privacy Policy (LC6).
- New Zealand Government Cloud Computing Risk and Assurance Framework.