CLOUD & INTERNET SERVICES POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	August 2016
Next Review	August 2019
Approval	SLT 16/08/161
Effective Date	August 2016

Purpose:

Cloud and Internet Services can provide fast or convenient delivery of information technology services. The purpose of this policy is to ensure that when such services that are adopted, that they comply with the information security requirements of the University in order to:

- Protect the availability, integrity, and confidentiality of institutional data.
- Reduce the risk that institutional data will be deliberately or inadvertently stored or transmitted, where it can potentially be accessed by unauthorised parties.
- Ensure compliance with legislative requirements.

Audience:

All University staff or anyone performing work on behalf of the University (including contractors, consultants, volunteers, and students conducting research on behalf of the University) are subject to this policy.

Scope:

This policy covers internet-based Cloud Services used to store, transact, transmit or process Massey University data.

Policy:
- Massey University provides facilities for secure transmission, processing and storage of data and information; however it is recognised that there may be instances where staff need to use non-University owned Cloud Service facilities. These services include, but are not limited to:
    - o Internet Services such as Facebook, Twitter, and Non-Massey University provided email.
    - o Software as a Service (SaaS) applications used to store or modify University data on non-University owned facilities and applications such as Project Management, Customer Relationship Management, Google Docs, Dropbox, or iCloud.
    - o Cloud Services such as Microsoft Azure or the New Zealand Government Cloud Programme which offers services via a pay-as-you go or subscription based model.
- Use of Cloud and Internet services must comply with all other University policies and relevant legislation.
- It is the responsibility of staff procuring such services to ensure that they are aware of, and comply with;
    - o the relevant end-user or terms of use agreements from the service provider;
    - o University financial delegations, as all costs incurred by the user are charged to their Budget Centre;
    - o information security policies, procedures, and relevant legislation; and
    - o security protocols normally used in the management of University data (on conventional storage infrastructure) are applied when storing and accessing such resources on Cloud Services.
- ITS will provide advice and consultation services in relation to the requirements outlined in this policy.

Definitions:

Availability	In information security, Availability is that component of information assurance that focuses upon providing immediate access to mission critical data when it is needed for decision making. It would, otherwise, negatively influence the organisation's productivity.
Cloud and Internet Services	Means services made available to users on demand via the Internet from a cloud computing provider's servers, as opposed to being provided from Massey's own on-premises servers.
Confidentiality	In information security, Confidentiality refers to the condition under which all information, software, and infrastructure remains private.
Conventional Storage Infrastructure	The data storage technology employed at Massey University premises to store, manage and protect data and information. This could be mapped network drives, staff intranet website, or information stored in an application that is only available to authorised staff.
Information Security	Directly relates to providing for the confidentiality, integrity and availability of all digital resources for Massey University. This provides assurance that information is only accessible by those who are authorised to view it, records and data are valid and correct, and mission critical information is accessible when it is needed.
Integrity	In information security, Integrity is the component of information assurance that relates to the validity and reliability of all of the information assets. The word itself directly relates to the accuracy of the data records used for processing and decision making as well as the adherence to a process that guarantees the precision of the data.
Security Policies	Refers to information security policies accepted and adopted by Massey University.
Software as a Service	Or SaaS, is a software licensing and delivery model in which software is licensed on a subscription basis and is hosted by a third-party. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users via a web browser.

Audience:

All staff

Relevant legislation:

- Privacy Act 1993

Legal compliance:

- Privacy Act 1993
  Establishes a set of privacy principles to ensure the protection of personal privacy in respect of both public and private sector organisations. The Act is of prime importance and should be clearly understood by all information management professionals.

Related policy and procedure compliance:

Information Security Policy
Endpoint Device Policy
Privacy Policy
Internet Use and Digital Communications Policy
User Code and Password Policy
Data Network Policy
Telecommunications Policy

Related procedures / documents:
Massey University Information Security Manual
ISO/IEC 27000:2014 – Information technology – Information security management systems
Information Security @ Massey University

Document Management Control:
Prepared by: Information Technology Services
Authorised by: The Chief Information Officer
Approved by: SLT 16/08/161
Date issued: August 2016
Last review: August 2016
Next review: August 2019