MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA

sUNIVERSITY OF NEW ZEALAND

# SECURE CLOUD PROCUREMENT & USE POLICY

| | |
|---|---|
| **Section** | Information Technology Services |
| **Contact** | Chief Information Officer |
| **Last Review** | January 2021 |
| **Next Review** | January 2024 |
| **Approval** | SLT 21/02/18 |
| **Effective Date** | August 2016 |

## Purpose:

Massey University is committed to the security of the University's Information Technology (IT) systems and data while enabling employees to carry out their jobs as efficiently as possible through the use of different technologies. The following policy and guidelines outline how end users can procure and use cloud services in a secure manner without compromising University data, IT systems, or the ability to conduct business.

- Ensuring the security, privacy and ownership rights of University information held by cloud service providers is appropriate, clearly specified and are built into the contractual arrangements for that service.
- Risk identification and mitigation that ensures institutional data will not be deliberately or inadvertently stored or transmitted, where it can potentially be accessed by unauthorised parties.
- Participating via the formalised vendor management program that manages supplier transparency to reduce risk exposure across the supply chain.
- Ensuring compliance with other relevant Massey policy and legislative requirements.

## Policy:

This policy applies to all University staff or anyone performing work on behalf of the University (including but not limited to contractors, consultants, volunteers, and students conducting research on behalf of the University) who procure or commission services that propose to use outsourced or cloud service provider services.

This policy applies to all business processes and data, information systems and components, and physical areas of the University. It includes all cloud services, all cloud-based email, document storage, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) etc. Employee personal cloud accounts are excluded.

## Policy Statements:

1. The **Vice-Chancellor** has the overall responsibility for the confidentiality, integrity, and availability of corporate data.
2. The **Chief Information Officer** has delegated execution and maintenance of information technology and information systems.
3. The **Associate Director, ITS Security, Risk, Information & Records** will provide advice in relation to the requirements outlined in this policy.

4. It is the responsibility of staff procuring such services to ensure that they are aware of, and comply with;
   - the relevant end-user or terms of use agreements from the service provider
   - University financial delegations, as all costs incurred by the user are charged to their Budget Centre
   - information security policies,procedures, and relevant legislation, and
   - security protocols normally used in the management of University data (on conventional storage infrastructure) are applied whenstoring and accessing such resources on Cloud Services.

**Cloud Procurement Guidelines**

Any end users, working groups, or departments looking to use cloud services for either single project based work or ongoing work, must follow these guidelines:

1. The use of cloud services must adhere to existing University security policies

2. The use of cloud services handling Massey University information or data must be authorized by the Chief Information Officer (CIO). A Cloud Risk Assessment to determine if security, privacy, availability, and other IT requirements are being adequately met must be completed. The approving Data Custodian is ultimately responsible for the risk inherent of the cloud services that they choose.

3. Individual end users are not permitted to open cloud service accounts or enter into cloud service contracts that will initiate a new vendor relationship, manipulate, or change existing relationships without the direct approval and input from the CIO.

4. For any cloud services that require individual users to agree to terms of service or usage, the office of the CIO will review such documents and determine if end users can agree on an individual basis or identify any needed changes. Always check with ITS, Security to see if any terms of service or usage you are agreeing to have been reviewed.

5. Personally owned and managed cloud services may not be used for work-related purposes including the storage, management, manipulation, sharing, or exchange of company related or owned data.

6. Any usage of cloud services must include a data backup schedule. This is in effect to secure Massey's ability to continue operations in the event a cloud service provider is unable to continue service.

**Information Security Classification and Encryption**

1. All information moving to and through Massey University's usage of cloud services is subject to and must adhere to the University's Information Security Classification Policy and Framework.

2. If at any point the flow of data will contain SENSITIVE information, such as, personally identifiable information (PII), credit card numbers, confidential or any other sensitive or regulated data, the data must be encrypted before being moved to a cloud environment.

3. Any usage of cloud services must adhere to all applicable laws and regulations governing Massey University.

## Definitions:

**Availability** in information security, 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 Risk Assessment** is a comprehensive overview of the cloud application and the risk the application poses to data.

**Cloud 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** means 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 Classification** in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data determines what baseline security controls are appropriate for safeguarding that data. Massey University has three sensitivity levels, or classifications: UNCLASSIFIED; IN CONFIDENCE; SENSITIVE.

**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.

**Infrastructure as a Service** or IaaS, refers to solutions that provide services such as storage, virtual server hosting, networking, or other infrastructure components via the internet.

**Integrity** in information security, 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.

**Platform as a Service** allows users to develop, run and manage applications without building and maintaining infrastructure. PaaS provides methods to interact with services like databases and file storage, without having to deal with low level requirements.

**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.

## Relevant Legislation:

Privacy Act, 1993.

## Legal compliance:

Privacy Act 1993

Establishes a set of privacy principles to ensure the protection of personal privacy inrespect 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:

Acceptable Use of Technology
Information Security Classification Policy
Information & Technology Security Policy
Desktop Hardware and Software Acquisition Policy
Device Security Policy
Password Policy
Privacy Policy
Procurement Policy
Telecommunications Policy

## Related procedures / documents:

Massey University Information Security Manual
ISO/IEC 27000:2014 –Information technology

## Document Management Control:

| | |
|---|---|
| Prepared by: | Chief Information Officer |
| Authorised by: | Deputy Vice Chancellor, Finance and Technology |
| Approved by: | SLT 21/02/18 |
| Date issued: | August 2016 |
| Last review: | January 2021 |
| Next review: | January 2024 |