SECURE CLOUD PROCUREMENT & USE 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

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

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