1. Background

This guideline highlights important considerations when utilising cloud services and will assist UNSW meet its obligations under the Data Governance Policy, Research Data Governance & Materials Handling Policy, Privacy Policy, Recordkeeping Policy and the IT Security Policy – Information Security Management System (ISMS).

The National Institute of Standards and Technology (NIST) defines cloud computing as ‘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’.

The three typical service models for cloud computing are:

- **Software-as-a-Service (SaaS)** – a software licensing and distribution model where a service provider hosts applications for customers and makes them available on a subscription basis over the internet. An example at UNSW would be PageUp within HR.

- **Platform-as-a-Service (PaaS)** – a service model where a service provider delivers a platform to customers, enabling them to develop, run, and manage applications without the need to build and maintain their own software development infrastructure. An example at UNSW would be the Microsoft Azure environment.

- **Infrastructure-as-a-Service (IaaS)** - a service model where a service provider hosts hardware equipment, operating systems and other software, servers, storage systems, networks, and other fundamental computing resources to enable a customer to deploy and run software, which can include operating systems and applications. An example at UNSW would be the Amazon Web Services (AWS) environment.

Cloud services can enable flexible and rapid delivery of applications and services and there are significant potential benefits for UNSW. However, the increased adoption and use of cloud services requires careful planning and management to reduce data handling and information security risks.

2. Guidance

2.1. Selection and Sourcing

Contact UNSW IT to determine if your business requirement can be met through an existing Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS) offering.

Where the business requirement cannot be met through an existing service offering, users should first determine if a UNSW supplier or UNSW panel supplier can deliver the required services, in accordance with the Procurement Policy.

If there are no UNSW suppliers or UNSW panel suppliers that can deliver the required services, the Procurement Procedure provides clear guidance on the processes to be followed based on the estimated total cost of the service. Contact UNSW IT to ensure that the selection of a potential cloud
service provider supports the university’s broader strategic technology objectives and meets the obligations for data governance and information security.

2.2. Data Governance and Information Security

Institutional data is a strategic asset of UNSW and the appropriate governance for management and use of data is critical to the University’s operations. Lack of governance can lead to operational inefficiencies and could expose UNSW to unwanted risks. This is particularly true for the adoption and use of cloud services.

The Data Governance Policy, Research Data Governance & Materials Handling Policy and IT Security Policy – Information Security Management System (ISMS), with their related Standards and Guidelines, outline the principles and minimum standards that guide the University’s data and information governance and information security procedures.

At a minimum, all Systems or Services must address the requirements of:

- Data Classification Standard
- Data Handling Guidelines
- IT Security Standards
- ITSS_21 IT Security Standard – Secure Algorithm List (SAL)

And specific to cloud services:

- ITSS_07 IT Security Standard – Cloud Computing Security

All cloud services that will hold or process personal information on behalf of the University must:

- be subject to a Privacy Impact Assessment prior to the implementation of the service to ensure such information is protected from unauthorised access, use, modification or disclosure of the personal information;
- be governed by a binding contract or agreement that sets out the rights and obligations of the Cloud Service Provider (CSP) and the University in regard to the management of the personal information.

2.3. Practical Considerations

To assist with understanding how to apply the relevant Policies, Standards and Guidelines in practice, before engaging a cloud service provider the following needs to be considered:

- In accordance with the Cloud Computing Security Standard, cloud services can only be consumed following a formalised risk assessment to identify the necessary security controls that must be established by the Cloud Service Provider (CSP) and UNSW to manage security risks to an acceptable level. Contact UNSW IT for assistance.

- Once data has been classified in accordance with the Data Classification Standard, the Data Handling Guidelines describe the practices that must be applied through all stages of the data lifecycle, including the implications for data sovereignty and data storage which are particular concerns for cloud services. Contact UNSW Planning & Performance for assistance.

- The Secure Algorithm List (SAL) provides further guidance on the use of cryptography and encryption for cloud hosted systems based on the relevant data classification. Contact UNSW IT for assistance.

- The Cloud Security Standard provides further guidance on obligations for contracting with CSP’s, including the requirements for ensuring that business continuity and disaster recovery plans meet UNSW requirements. Contact UNSW IT for assistance.

- In accordance with the Recordkeeping Policy, records and information management requirements need to be identified and assessed when entering into cloud, or similar, service arrangements. Contact the UNSW Manager, Records & Archives for assistance and guidance on recordkeeping requirements.

- Contact the UNSW Privacy Officer for assistance with Privacy Impact Assessments and guidance on contractual requirements for the protection of personal information.
### Accountabilities

<table>
<thead>
<tr>
<th>Responsible Officer</th>
<th>Chief Digital Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Officer</td>
<td>Director, Business IT Services (Interim)</td>
</tr>
</tbody>
</table>

### Supporting Information

<table>
<thead>
<tr>
<th>Legislative Compliance</th>
<th>This Guideline assists the University’s compliance with the following legislation: Nil</th>
</tr>
</thead>
</table>
| Parent Document (Policy and Procedure) | Data Governance Policy  
|                        | Research Data Governance & Materials Handling Policy  
|                        | IT Security Policy – Information Security Management System (ISMS)  
|                        | Procurement Policy |
| Supporting Documents   | Nil |
| Related Documents      | Data Classification Standard  
|                        | Data Handling Guidelines  
|                        | ITSS_07 IT Security Standard – Cloud Computing Security  
|                        | ITSS_21 IT Security Standard – Secure Algorithm List (“SAL”)  
|                        | IT Security Standards  
|                        | Procurement Procedure |
| Superseded Documents   | Nil |

| File Number | 2020/002074 |

### Definitions and Acronyms

**Cloud Services**

The on-demand delivery of computing services over the Internet – including servers, storage, databases, networking, software, analytics and intelligence. Typically characterised by paying only for the cloud services you use.

**Software-as-a-Service (SaaS)**

A software licensing and distribution model where a service provider hosts applications for customers and makes them available on a subscription basis over the internet.

**Platform-as-a-Service (PaaS)**

A service model where a service provider delivers a platform to customers, enabling them to develop, run, and manage applications without the need to build and maintain their own software development infrastructure.

**Infrastructure-as-a-Service (IaaS)**

A service model where a service provider hosts hardware equipment, operating systems and other software, servers, storage systems, networks, and other fundamental computing resources to enable a customer to deploy and run software, which can include operating systems and applications.

### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Approved by</th>
<th>Approval date</th>
<th>Effective date</th>
<th>Sections modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Vice-President, Finance and Operations</td>
<td>20 December 2019</td>
<td>20 December 2019</td>
<td>This is a new Guideline</td>
</tr>
</tbody>
</table>