THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Information Technology Instruction:

Cloud Computing Software as a Service

Effective: 23 October 2023

Audience: Employees, Students

Key words:	Cloud, software, data, information, information security
Instruction Owner:	Chief Information Officer
Responsible Officer:	Director, IT Business Partners & Security
Review Date:	23 October 2024

Information Technology Instruction: Cloud Computing Software as a Service

1. Authority and force of this instruction

The *Policy: Information and Information Technology* authorises the Chief Information Officer (CIO) to maintain detailed instructions for staff to ensure security of the University's information (clause 5.3.1.2).

The *Procedure: Information Management* authorises the CIO to maintain instructions for staff to ensure 'secure use of university-provided software' (clause 12.4.2).

2. Instruction

2.1. This instruction supplements the *Procedure: Procurement* by stating additional requirements specific to procurement of cloud computing services and software as a service (SAAS). Staff should read this instruction alongside the *Procedure: Procurement*.

Scope

2.2. This instruction applies to all staff involved in deciding whether to engage a third-party organisation to provide cloud computing or SaaS to the University.

Initial discussion with IT Business Partner

2.3. Any staff member who is considering engaging a third-party organisation to provide cloud computing or SaaS, or to use a new service from a already approved supplier of cloud computing or SaaS, must first discuss this with the IT Business Partner of their organisational unit.

First step in engaging a third-party provider of cloud computing or SaaS

2.4. Regardless of the cost of a proposed engagement of a third party to provide cloud computing service or SaaS, the engagement request must first be submitted to the IT Business Partner of the organisational unit that is requesting the engagement.

Assessment of third-party providers

2.5. Procurement maintains the questionnaire for potential suppliers, to inform assessment of whether they are suitable to be used.

2.6. In collaboration with Procurement, the Director, IT Business Partners and Security will maintain a supplementary questionnaire for possible third-party providers of cloud computing or SaaS (the UNDA Supplier Questionnaire), to inform decisions whether:

- the third party is reputable and will be able to provide the service for the period when the University will need it
- the third party's information security and quality assurance processes are sufficient to ensure satisfactory service, continuity of service and security of the University's information that will be created or held by the third party, and
- the third party may store university information in countries where there are greater risks to security and privacy of university information.

2.7. In assessing a third-party provider of cloud computing or SaaS, Information Technology may, in consultation with Procurement, accept, in place of answers to information security questions in the assessment questionnaire:

- satisfactory industry certification of the provider's information security measures, and/or

- the provider's inclusion on a white-list of safe providers maintained by a Commonwealth or state government department.

2.8. The CIO holds the delegations to approve commissioning and operation of outsourced cloud computing and online services; the Chief Financial Officer (CFO) holds the delegation to approve suppliers and contracts with suppliers.

- Accordingly, for a proposed supplier of cloud computing or SaaS, the CIO endorses the recommendation to approve the supplier, for the CFO's approval.

2.9. Information Technology, in collaboration with Procurement, may pre-assess third-party organisations as satisfactory to provide a cloud computing service and/or SaaS, so that Procurement can list them as pre-approved for engagement to provide a specific range of services.

- Staff whose units need a supplier of a cloud computing service or SaaS are expected to engage a listed supplier if practicable.

Contracts

2.10. The Director, IT Business Partners and Security, in collaboration with Procurement, will ensure that contracts with third-party providers of cloud computing services or SaaS include conditions to ensure:

- satisfactory service, continuity of service and security of the University's information created or held by the third party
- processes to detect, record and report to the University security-related events
- processes to monitor for, report to the University and resolve incidents and defects, and to ensure disaster recovery
- privacy, non-disclosure of university information, and proper assignment of intellectual property, and
- where the arrangement will involve a high level of risk for the university, a process for the University to audit, at least annually, whether the third party is meeting the conditions. (However, continued industry certification may be accepted in place of aspects of these audits.)

High-risk arrangements

2.11. The Director, IT Business Partners and Security will decide, in consultation with Procurement, whether an arrangement with a third party to provide a cloud computing service or SaaS has a high level of risk for the University, on criteria such as whether the service:

- is essential to maintaining continuity of the University's core business, and/or
- involves the third party holding or generating university information that is classified as sensitive or very sensitive: see the Information Management Procedure for these classifications.

Once contracts are in effect

2.12. A third-party provider of a cloud computing service or SaaS will not be given access to facilities or data of the university until there has been an initial evaluation of the provider has been completed and a contract for the services is in effect.

2.13. Staff configuring a cloud computing service or SaaS software for use at the University will ensure that it is configured to avoid vulnerabilities: for example, so that

- passwords – particularly those of system administrators – are of a strength required to access the University's own information systems, and

- any documents stored using the service are only accessible to users located in Australia.

2.14. Where the Director, IT Business Partners and Security has classified an arrangement for third-party provision of a cloud computing service or SaaS as high risk, the director will ensure that the arrangement is reviewed at least annually to assess whether the risks are being adequately managed.

Register of providers

2.15. Procurement, in collaboration with Information Technology, will maintain a register of third-party providers of cloud computing services or SaaS to the University.

2.16. The Director, IT Service Delivery and Operations also maintains a more detailed register of suppliers of cloud computing services and SaaS to the University, which includes the services that each currently provides.