IT Asset - Cloud Storage Procedure

Section 1 - Summary

(1) The purpose of this Procedure is to define Victoria University's (VU) position on the use of cloud storage and similar services for the storing and sharing of VU data and information.

Section 2 - TEQSA/ASQA/ESOS Alignment

(2) HESF: Standard 2.1 Facilities and Infrastructure, 7.3 Information Management.

(3) Outcome Standards for NVR Registered Training Organisations 2025: Standard 1.8 Facilities, Equipment and Resources.

Section 3 - Scope

(4) This Procedure applies to:

a. All VU staff and affiliates in all onshore and offshore locations who use cloud storage and sharing services in performing their work for VU.
b. Research activities undertaken by VU staff and research students using cloud services.

(5) This Procedure does not apply to departments or VU as a whole if considering the use of cloud storage systems in lieu of corporate IT systems. See IT Asset - Business Application Procedure.

(6) The Cloud Storage Procedure supports the IT Asset Policy and should be read in conjunction with the Information Security Policy and Records Management Policy.

Section 4 - Definitions

(7) Cloud storage: Web based file storage model that can be accessed with an internet connection and from multiple devices.

Section 5 - Policy/Regulation

(8) IT Asset Policy

Section 6 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibilities
Staff	Use the University's recommended cloud file sharing and storage solutions to store and/or share University files and data.
Researchers	Use services recommended for supporting research in preference to other cloud services.

Part B - Cloud Storage

University Cloud Storage Services

(9) VU provides all staff with access to a Microsoft Office 365 account which includes the use of cloud storage applications SharePoint, OneDrive for Business and Teams using their staff account details. This is the University's recommended cloud file sharing and storage solution for use by University staff to store and/or share University files and data. For the management of research data, see Research Specific Cloud Storage and Retention Guidelines below.

(10) Staff using a cloud file storage and sharing service other than the VU supported solution to store or share University files and data may increase the level of risk to the security of VU information and data.

(11) Where University data has been stored on another cloud storage solution, VU recommends migrating this data to the approved provider solution and permanently deleting the data from the previous location.

(12) The use of alternative cloud storage solutions to store and share University files and data must be approved by ITS and conform to the University's Purchasing Policy, Contracts Policy and undergo a full risk assessment to ensure the solution is fit for purpose, secure and cost-effective.

(13) Access to files and data stored on cloud storage applications will be provided based on business need and protected based on their classification and sensitivity in accordance with the Information Security Policy.

(14) Staff should follow the Best Practice Guidelines for Using Cloud Storage Safely when using cloud storage solutions to store, access or share VU information and data.

Personal Cloud Storage Accounts

(15) Accounts for cloud storage services setup by a staff member through a personal subscription are considered a personal account. This includes cloud storage, file synchronisation and sharing tools such as Dropbox™ and Google Drive.

(10) University files and data including business critical, sensitive or highly sensitive University information should not be stored on a staff member's personal cloud data storage service. Staff will not use personal accounts or other cloud storage tools to store or share:

a. Official statements or positions;
b. Private or confidential information of others;
c. Sensitive data including commercial in confidence, legal documents and some types of sensitive research data;
d. Financial information, budgets and strategic plans or internal audit reports;
e. Information covered by the Health Records Act 2001 (Vic) including all health information disclosed to VU, regardless of context (e.g. information disclosed to VU's Counselling and Disability Services, health information disclosed in a VU clinic or teaching facility).

Research Specific Cloud Storage and Retention Guidelines

(16) A number of cloud services exist specifically for supporting (Australian) research and these should be used in preference to other cloud services where practical. These include:

a. CloudStor Plus - for researchers to store and share data online with collaborators.
b. CloudStor File Transfer - for sending and receiving of larger files.
c. NeCTAR - hosted cloud infrastructure allows development of custom solutions which may house data. National virtual laboratory infrastructure is generally hosted here.
d. RDSI or VicNode - nationally funded storage infrastructure generally for large datasets.

(17) Research staff and students must meet their professional responsibilities set out under the Australian Code for the Responsible Conduct of Research (2018) (Cth), the VU Research Integrity Policy and any applicable responsibilities resulting from ethics, funding body or contractual obligations and legislation such as the Defence Trade Controls Act 2012 (Cth).

(18) Activities under an ethics application are required to detail where data will be kept, so the use of cloud storage must be approved or an ethics amendment must be sought. Research staff will avoid using cloud services to store identifying, private, personal, sensitive or potentially harmful information.

(19) Primary copies of research data and records must be kept safe, secure, and retained beyond the research activity in accordance with the Records Management Policy.

(20) The VU Research Data and Materials Plan form can be found on the VU Research Data Management webpage and helps projects to identify and document obligations, storage locations and retention requirements.

(21) Staff will avoid using the cloud as a primary copy, or alternatively, backup cloud data to a secure location regularly. VU provides the research network storage drive to aid researchers in retaining safe and secure data and records, both during projects and for the required retention periods.

(22) Before implementing any alternative cloud storage solution, staff will ensure to read and fully understand the implications and responsibilities in relation to a project and the data that will be supported by the solution.

Service Support

(23) The use of externally provided cloud storage cannot be supported by ITS.

Status and Details

Status	Current
Effective Date	18th March 2021
Review Date	15th March 2026
Approval Authority	Vice-President, Resources and Precincts
Approval Date	9th March 2021
Expiry Date	Not Applicable
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services +61 3 9919 5576
Enquiries Contact	Rebecca Xuereb Senior Project and Administration Officer rebecca.xuereb@vu.edu.au