IT Hardware and Software - Cloud Personal Storage Guidelines

Section 1 - Purpose / Objectives

(1) Cloud Personal Storage Guidelines provides information on the use of cloud storage services by individuals at Victoria University (VU).

(2) Cloud Personal Storage Guidelines supports the IT Hardware and Software Policy.

(3) This Guideline should be read in conjunction with the Information Security Policy and Records Management Policy .

Section 2 - Scope / Application

(4) This Guideline applies to:

a. All VU staff and affiliates who wish to use external file synchronisation and sharing (cloud storage services) tools in performing their work for VU.
b. How the tools can be used by staff and the types of data which can be shared with limited risks to VU's information assets.
c. Research activities undertaken by VU staff and research students using cloud services.

(5) This Guideline 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 Cloud and Managed Services Procedure .

Section 3 - Definitions

(6) Nil

Section 4 - Policy Statement

(7) Nil

Section 5 - Procedures

(8) Nil

Section 6 - Guidelines

Part A - Cloud Storage Services

(9) Cloud style services can be used for information processing, file synchronisation and external file sharing. Tools providing these services may include Dropbox™, Google Drive, Box, Amazon, ExactTarget, Yammer S3 or other file synchronisation and sharing services.

(10) The Victorian Information Commissioner has provided guidance around the use of cloud computing services. Advice around the record keeping implications of cloud storage has also been prepared by Public Record Office Victoria. Cloud computing providers must comply with the Victorian Information Privacy Principles, in particular IP4: Data Security.

Part B - Benefits and Limitations/Risks

(11) Cloud storage solutions may be useful for improved efficiency and collaboration with external parties, but may also significantly increase the level of risk to the security of VU information and data.

(12) Benefits of Cloud Storage Services:

a. Efficient sharing of large files, presentations and notes with yourself (synchronisation across many devices), other staff, visitors and external partners which can be limited to specified folders or files.
b. Basic collaboration tools allowing multiple people to work on the same document simultaneously.
c. Reduction in the use of email attachments and associated storage.
d. Easy-to-use free solutions, usually with storage limited to a few gigabytes and options to quickly scale to paid services which offer more storage and greater functionality.
e. Simplifies collaboration among researchers within the University and across different institutions.

(13) Limitations and Risks of Cloud Storage Services:

a. The ease of file sharing can result in the inadvertent sharing of files.
b. Saved files may automatically save to other devices and websites.
c. The vendor website retains copies of all information - even if you delete your files.
d. Any file deleted on one device may be retrieved from a synchronised device through the service.
e. Some organisations may not allow collaboration using cloud storage services.
f. Service outages may be unannounced and may be temporary or permanent.
g. In some cases, cloud storage providers may be able to access or have joint ownership over the files you have uploaded.
h. Terms and conditions of the cloud service may change over time.
i. New start-up companies offering free services may not have a proven business model and may therefore be susceptible to failure/closing down.

Part C - Risk Analysis

(14) Individuals considering using cloud storage services should perform a Risk Analysis (see Appendix 1) to assess the risks involved and ensure the type of data that you intend to transfer/share is suitable for cloud storage based solutions.

Part D - Staff Responsibilities and Considerations

(15) On completing the Risk Analysis, if the staff member determines that the use of a file synchronisation and sharing service or cloud based application for personal or project working data is suitable, the staff member must take a

number of considerations into account (see Appendix 2).

(16) The staff member is responsible for researching the chosen service or application and agrees to take these considerations (Appendix 2) into account when enabling a file synchronisation or sharing service or using a Cloud based application for personal or project working data.

(17) Please note that storing personal information using a cloud based service can also lead to identity fraud. Caution needs to be exercised on the type of personal data stored in the Cloud. The staff member is responsible for accepting the risks associated with storing this type of data in a cloud based storage solution.

Part E - Research Specific Cloud Storage Guidelines

(18) 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 with collaborators. This service is similar to DropBox.
b. CloudStor File Transfer - for sending and receiving of large files, essentially super-sized email attachments. This service is similar to YouSendIt/Hightail or WeTransfer.
c. NeCTAR - hosted cloud infrastructure allows development of custom solutions which may house data. National virtual laboratory infrastructure is generally hosted here. This service is similar to Amazon EC2, S3 or Google Cloud Platform.
d. RDSI or VicNode - nationally funded storage infrastructure generally for large datasets.

(19) Research staff and students must meet their professional responsibilities set out under the Australian Code for the Responsible Conduct of Research, the VU Research Integrity Policy and any applicable responsibilities resulting from ethics, funding body or contractual obligations.

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

(21) Primary copies of research data and records must be kept safe, secure, and retained beyond the research activity. Avoid using the cloud as your primary copy, or alternatively, backup cloud data to a secure location regularly. VU provides the research storage (the R: drive) to aid researchers in retaining safe and secure data and records, both during projects and for the required retention periods. The VU Research Data and Materials Planning form can be found on the VU Research Data Management webpage and helps projects to identify and document obligations, storage locations and retention requirements.

(22) Before implementing any solutions that enable this type of service, ensure you read and fully understand the implications and your responsibilities in relation to your project and the data that will be supported by the solution.

Part F - Service Support

(23) Technical support and user assistance for these types of solutions are limited to that which is available from the service provider being utilised. It is your responsibility to ensure you can get the correct level of assistance required.

(24) The use of cloud storage services cannot be fully supported by ITS given the service is engaged by VU employees through a personal subscription.

Status and Details

Status	Historic
Effective Date	20th May 2015
Review Date	31st December 2019
Approval Authority	Vice-Chancellor
Approval Date	21st January 2015
Expiry Date	17th March 2021
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Enquiries Contact	Jessica Carter Coordinator Quality Assurance +61 3 99196292