IT Hardware and Software - Cloud Storage Guidelines

Section 1 - Purpose / Objectives

(1) The guideline specifies 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. The guidelines should be read in conjunction with the Information Security Policy and Records Management Policy.

Section 2 - Scope / Application

(2) 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. Such tools may include Dropbox™, Google Drive, Box, Amazon, ExactTarget, Yammer S3 or other file synchronisation and sharing services. These tools may be appropriate for individual convenience and collaboration.
b. Research activities undertaken by VU staff and research students using cloud services. See the below section for research specific guidelines.

(3) This guideline does not apply to departments or VU as a whole if considering use of cloud storage systems in lieu of corporate IT systems. In this case, a full procurement process must be undertaken, including a full risk assessment and consideration of options. Consultation with the IT Security and Assurance team, the Records Services team, and the provision of Legal advice from Legal Services must be undertaken.

(4) It should be noted that external file synchronisation and sharing tools cannot be fully supported by the University Information Technology Services department given the service is engaged by VU employees through a personal subscription.

Section 3 - Definitions

(5) Nil

Section 4 - Policy Statement

(6) Nil

Section 5 - Procedures

(7) Nil

Section 6 - Guidelines

(8) Cloud style services can be used for information processing, file synchronisation and external file sharing. These 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.

(9) The Victorian Privacy 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 A - Benefits and Risks

(10) Cloud storage services benefits include:

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.

(11) There are also limitations and risks:

a. The ease of file sharing can result in the inadvertent sharing of files.
b. Saved files automatically save to other devices and the website.
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 and innovative start-up companies offering free services without a proven business model.

Part B - Types of information that can readily be used in these services

(12) Acceptable low risk information holdings that can be transferred and shared using a cloud service include:

a. Your own personal data and notes

Staff responsibilities for enabling a file synchronisation or sharing service or using Cloud based applications

(13) If staff determine a requirement for the use of a file synchronisation or sharing service or Cloud based application for personal or project working data, the following considerations should be taken into account:

a. How much data will be placed in the cloud? For limited data sets, a free service may provide efficient storage.

For larger amounts of data, you may need to purchase storage.

b. Data that can be moved to the cloud should not be business critical and should be either personal data or working data and not bound by IP or contractual agreements.
c. You will need to maintain an up-to-date off-cloud backup copy of the data.
d. Ensure that the Service Level Agreement (SLA) guarantees adequate system confidentiality, integrity and availability of the data. For example, an acceptable level of data unavailability is 4 — 6 hours.
e. There will be scheduled outages that you need to accept.
f. If you accidentally delete a file or other data, can the vendor restore it?
g. Can you easily move the data to another vendor or in-house as required?
h. You accept the privacy laws of countries that have access to your data. You also need to adhere to Victoria's Privacy Act as well — the Victoria Privacy Commissioner has provided advice about the use of cloud computing and cloud computing suppliers should comply with Victoria's Health Records Act.
i. You need to retain legal ownership of your data.
j. Ensure the vendor is contactable and provide timely responses and support.
k. Ensure the vendor will notify you of security incidents and you will monitor and respond to these notifications.

(14) For research activities obligations regarding the management of research data still apply. See the below section for research specific guidelines.

Part C - Research Specific Guidelines

(15) 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 file, 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.

(16) Research staff and students must meet their professional responsibilities, namely the Australian Code for the Responsible Conduct of Research, the VU Research Integrity Policy, any associated ethics or legal requirements, funding body or contractual obligations.

(17) 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.

(18) 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.

(19) 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 D - Service Support

(20) 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.

Part E - Risk Analysis

Data	Risk	What is at risk	Risk to	Mitigations
Personal and reference information — working information, reference material	Negligible	Nothing	Personal data belonging to VU staff	User accepts the risk of storing this data in a cloud based storage solution.
Project / working data (non-commercial and not sensitive)	Low	Availability	Staff being able to access data for projects they are working on	Project leader accepts the risk that their data may not be available at a critical time during the project.
Information covered by the Information Privacy Act 2000	Medium	Confidentiality	Information covered by the Information Privacy Act 2000 - personal identifying information, job applications, HR and medical data etc. Includes student personal information and progress or grievance issues.	Cloud storage providers must comply with the Victorian Information Privacy Principles, particularly IP4 Data
Official data	Medium	Integrity and Availability	Reputation of VU if the data is altered or if it is unavailable for the public to access	Do NOT use cloud based storage solutions. Further investigation into these services is ongoing.
Freedom Of Information (FOI)	Medium to High	Confidentiality and Integrity	Reputation to VU if the data is altered or accessed by non-authorised people (this would be around personal FOI data). Legal issues may arise if personal data was accessed inadvertently.	Do NOT use cloud based storage solutions. Further investigation into these services is ongoing.
Sensitive data including commercial in confidence and some types of research data	High	Confidentiality, Integrity and Availability	Reputation to VU, could impact on funding, inadvertent access to or released of data.	Do NOT use cloud based storage solutions. Further investigation into these services is ongoing.
Financial data	High	Confidentiality, Integrity and Availability	Financial impact, if funding could be accessed, through either Commercial research companies being able to underbid or an attacker being able to commit fraudulent activities.	Do NOT use cloud based storage solutions. Further investigation into these services is ongoing.

Information covered by the Health Records Acts 2001	High	Confidentiality and integrity	Reputation to VU if the data is altered or accessed inadvertently. Legal issues may arise if health data was accessed or released. Includes all health information disclosed to VU, regardless of context (eg information disclosed to VU's Counselling and Disability Services, health information disclosed in a VU clinic or teaching facility).	Do NOT use cloud based storage solution. Further investigation into these services is ongoing.

Part F - References

(21) This document was developed using CSIRO guidelines provided to the Council of Australian Universities Directors of Technology.

(22) Victorian Privacy Commissioner, "Cloud Computing Information Sheet".

Status and Details

Status	Current
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	Vice-Chancellor
Approval Date	To Be Advised
Expiry Date	Not Applicable
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