Typical Risks on Using Public Cloud Services

Below is a list of typical risks associated on using public cloud services like Dropbox, GoogleDocs, OneDrive, etc.

Typical Risks on Using Public Cloud Services

Typical Risk Events			Probability	Notes on Potential Impact/Consequence
Context	**System**	**Process**	**Frequency**	
		Records and Information security misclassified	Almost Certain *(More than once per year)*	The consequence of misclassification of records and information could lead to other risk events that range from insignificant to severe and also dependent on the information's sensitivity and confidentiality. See: Information Security Classification Policy and Procedures and Decision Framework on the Use of Cloud Services for more information
Changes to the Australian Privacy Principles			Possible *(At least once between 1 & 5 years)*	Consider if the changes affect security and access restrictions, usage of cloud service, etc.
Phishing emails targeting users of Dropbox, OneDrive, GoogleDocs, etc.		Unauthorised access with malicious intent	Almost Certain *(More than once per year)*	Phishing emails targets all personal valuable information – name, date of birth, bank account numbers, credit card numbers, user names, passwords, etc. For example, Google accounts can be used to access many services including Gmail & Google Play which can be used to purchase applications and content, etc. *(For more information on how to protect yourself from phishing emails, see: https://cits.curtin.edu.au/staff/info_sec/emailscammers.cfm)* Confidentiality of personally identifiable student & staff information might be compromised which leads to breach of the Privacy Act. Confidentiality of commercial information might be compromised which could lead to financial loss or damage to Curtin brand To minimise these risks, consider doing the following: 1. Set passwords and choose the appropriate "sharing" settings to ensure that only relevant people or only you have access to your Dropbox, OneDrive, etc. 2. De-identify data, i.e. remove any personal identifiable information 3. Encrypt your files (don't lose the passwords though) before storing them on the cloud See: Incident Alert Matrix and Curtin's Risk Reference Tables: Consequence Table – Interruption to Services for more information on how the University views these risks.
	Data loss due to system outage & technical obsolescence	Data loss due to accidental deletion	Almost Certain *(More than once per year)*	*1. Saving a copy of the information in Curtin systems minimises the impact of data loss* *2. Reconstruction cost for information has to be considered (cost of data, time and other resources needed to replace or reproduce the information)*

Please see the Decision Framework on the Use of Cloud Services and Frequently Asked Questions regarding Cloud computing for more information.