Curtin University

# TYPICAL RISKS ON USING PUBLIC CLOUD SERVICES

Below is a list of typical risks associated with using public cloud services such as Dropbox, GoogleDocs and OneDrive etc.

| TYPICAL RISK EVENTS | | | PROBABILITY | NOTES ON POTENTIAL IMPACTS / CONSEQUENCES |
|---|---|---|---|---|
| **Context** | **System** | **Process** | **Frequency** | |
| | | Records and information security misclassified. | Almost certain.<br>*(More than once per year).* | The consequences of misclassification of records and information could lead to other risk events that range from insignificant to severe, and is also dependent on the information's sensitivity and confidentiality.<br>For more information refer to: **Information Security Classification Policy and Procedures** and **Decision Framework on the Use of Cloud Services**. |
| Changes to the Australian Privacy Principles. | | | Possible.<br>*(At least once between 1-5 years).* | Consider if the changes affect security and access restrictions, usage of cloud services etc. |
| Phishing emails targeting users of Dropbox, OneDrive and GoogleDocs etc. | | Unauthorised access with malicious intent. | Almost certain.<br>*(More than once per year).* | Phishing emails target all personal valuable information, such as name: date of birth, bank account details, credit card numbers, user names, passwords etc. For example, Google accounts can be used to access many services including Gmail and Google Play, which can be used to purchase applications and content etc.<br>For more information on how to protect yourself from phishing emails refer to: **https://cits.curtin.edu.au/staff/info_sec/emailscammers.cfm**.<br>Confidentiality of personally information might be compromised which could lead to financial loss or damage to Curtin brand.<br>To minimise these risks, consider doing the following:<br>1. Set passwords and choose appropriate 'sharing' settings to ensure that only relevant people *(or only yourself)* have access to your Dropbox, OneDrive etc.<br>2. De-identify data, i.e. remove any personal identifiable information.<br>3. Encrypt your files *(don't loss the passwords though)* before storing them on the cloud.<br>For more information on how to manage these risks refer to: **Advice and assistance on Risk & Assurance at Curtin**. |
| | Data loss due to system outage and technical obsolescence. | Data loss due to accidental deletion. | Almost certain.<br>*(More than once per year).* | 1. Saving a copy of the information into Curtin systems will minimise the impact of data loss.<br>2. Reconstruction costs for information has to be considered *(cost of data, time and other resources needed to replace or reproduce the information)*. |

For additional information and advice, you may wish to refer to:

- Decision Framework of the Use of Cloud Services.
- Cloud Computing Frequently Asked Questions.
- Information Security & Risk Advisory Service.

## Need further assistance?

Please do not hesitate to contact us via phone on 9266 7050, or by email at: rim@curtin.edu.au, should you require additional support.

For information management advice of a general nature, please visit our website at: rim.curtin.edu.au.

This advice sheet is made under and supports the Information Management Policy and associated Procedures.