Cloud Storage Policy - Sample

Policy Brief and Purpose

The [Organization] is committed to ensuring its systems are secure, [Organization] data and systems are protected, and are only accessed by authorised users.

Scope

For this document, the phrase "cloud storage" refers to third party online storage services such as Google Drive, Dropbox and OneDrive. Files stored on these services can usually be accessed via any web browser and often have the capability to be "synchronised" to multiple computers and mobile devices such as mobile phone and tablets. They may also have facilities for sharing files with other people.

The scope of this policy includes all personnel who have or are responsible for
an account (or any form of access that supports or requires a password) on any system that resides at any facility, has access to the network, or stores any non-public information.

Risks

Many people are now using public cloud storage in their private lives. This allows convenient access to their files and data from a number of different devices. If employed in a work context however, such services also introduce risks to the security, privacy, copyright and retention of [Organization] data.

The main risks when files are stored in public cloud storage are that:

• The [Organization] can no longer guarantee the quality of access controls protecting the data
• In many cases, public cloud storage requires that files be associated with an individual's personal account. Should that individual suddenly become ill, be absent for other reasons or leave, the [Organization] will lose access to the data
• Cloud services generally limit their liability for negligence, resulting in little or no recourse should the provider
misuse, lose or damage information stored in the cloud
• Few cloud providers guarantee they will not access the information stored within their service, leading to concerns over privacy and intellectual property rights
• Some if not all providers do not guarantee that the user's ownership of the data stored in the cloud will be retained. This is primarily to enable the providers to move data around to their different server locations without your prior approval but opens further questions about intellectual property rights
• Using cloud storage client software to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment
• If they have financial difficulties a cloud storage provider may
end the service with little or no
notice, leaving users with no access to files

Policy Elements

• Do not use cloud storage to store files containing information about individuals or other sensitive information.

• Do not use cloud storage for the long-term retention of [Organization] documents or files even for instances when you work with non-sensitive information. Use alternatives such as SharePoint and shared network drives.
• The [Organization] does not support cloud storage clients or apps, such as those available for Dropbox.
• Do not store the only copy of a file in cloud storage
• You must ensure that there is a suitable level of encryption on any mobile or portable device used to download any data about individuals from cloud storage. Such a device must be password protected.