Using Cloud Storage Services Safely

For businesses looking to share resources quickly and effectively, cloud storage can be an attractive answer. Moving operations to the cloud is an effective way to reduce hardware and software costs while keeping data readily available. However, it can also expose your company to certain risks that you need to consider when deciding if this type of file storage is right for you.

How It Works

Cloud storage allows you to upload documents, videos, photos and other files to a website as backup copies and makes it easy to share those files with others. The files are accessible from any type of device (laptop, desktop, tablet, mobile phone, etc) in any location.

To use cloud storage, you first need to create an account with the service provider you choose. You will then create a folder on your computer for the files you want to back up or share. The files that are placed in this folder are copied to the storage provider's servers. If you make changes to a file within the folder, the file is automatically copied and the changes are instantly accessible from your other devices.

Most cloud services offer a limited amount of storage space for free. If you want a larger or unlimited amount of storage space, you typically have to pay a fee.

Storing and Sharing Files

Storing your files in the cloud means that the files are stored on servers controlled by the service provider. Some cloud service providers may even use the cloud services of another organisation to store your files. When choosing a cloud service provider, you should be sure that the service's security and availability are suitable for the types of files you will be storing.

The cloud can be used to store copies of important files outside of your business. Therefore, if you experience a disaster, such as a flood, you will have copies of your data and one less thing to worry about after the event. Storing files off-site is an important aspect of a business continuity plan.

Cloud storage also allows you to share files with others. The files can be shared and accessed across a range of devices and locations. It can sometimes be difficult to email large files such as photos or videos, but uploading them to the cloud allows you to send a URL and share files with anyone you choose.

Storing Personal Information

Before storing any personal information in the cloud, consider the following:

1. Who can access your files – Cloud storage services usually have three settings you can choose from that control who can view your files:
   - *Private* – You are the only one who can view the files. However, the cloud storage provider may also be able to view them.
   - *Public* – Anyone can view the files with no restrictions.
   - *Shared* – The people you invite to view the files are the only people who can see them.
2. The strength of your passwords – Your username and password control the accessibility of your stored files in the cloud. The password and username should be unique and difficult to guess. Do not use the same credentials for different sites. If one site is hacked, the attackers now have the credentials to access your other online accounts.
3. The storage provider's terms and conditions and privacy notice – Choose a cloud service provider that is transparent and honest about how your personal information will be secured and how they will or will not use it. Stay away from cloud services that either do not

provide this information or if you feel the terms are unclear or unreasonable.

4. The type of encryption the provider offers – Some providers store your data in an encrypted form and keep the key that can decrypt the files in a secure location. When you log in to the cloud, your files are decrypted and you can access them. Choosing a provider that manages the file encryption means you can invite other people to log in to your files, if that process works best for you.

   Your web browser can also encrypt files that you store in the cloud. The files are encrypted while they are being sent between you and the cloud, preventing them from being read or modified along the way. If your web browser is displaying a padlock symbol and the URL starts with 'https://', your files are being encrypted. Your files will be decrypted when the storage provider receives them. If you want your files to remain encrypted while in storage, encrypt them before sending them to the cloud, or choose a provider that will encrypt them for you.

5. If you can encrypt the files yourself – Encrypting your files before storing them in the cloud is the best way to keep your information safe and secure. If you are the only one with the encryption key, no one else will be able to decrypt your files and read your personal information. However, encrypting the files will prevent you from being able to share them with others without also sharing the encryption key—something to consider when determining how you will encrypt your information. Also keep in mind that if you lose or forget the key, you will not be able to decrypt your files.

   Encryption software tools are available for free or at a low cost on the Internet. However, when using software found online, make sure it comes from a trusted and reliable source, and check reviews to be sure the software has been tested and performs appropriately.

For more information about how to keep your data secure, contact Sentio Insurance Brokers Ltd today.