All cloud storage that you use must be protected by a strong passphrase and 2-Factor Authentication/Multi-Factor authentication (2FA/MFA). The most common cloud storage options (Google Drive or Microsoft One Drive) use their own default encryption while storing your documents/files on their premises, and tend to have full access to your information stored on their servers. Your files may also be requested by Governments and are vulnerable to the event of a breach. Using their specific email services means that all your incoming and outgoing emails are stored on the private companies’ servers as well. This information is vulnerable to “take downs” following requests by Governments or by companies own policies. The information stored on your office drives is as secure as the servers themselves (physically and digitally).

It is recommended to secure all your online cloud storage accounts by enabling 2-Factor Authentication/Multi-Factor Authentication (2FA/MFA). Adding 2FA/MFA on your cloud storages helps protect your cloud storage account against password attacks such as brute-force or credential stealing. 2FA/MFA should be enabled on all online accounts (including email) that offer this facility.

It is recommended to use an encryption tool (e.g. Cryptomator; or VeraCrypt). To encrypt your existing cloud storage if it does not come with built-in end-to-end encryption options. These software (paid or free, depending on the type of subscription,) allow you to encrypt multiple cloud storage accounts.

It is recommended to choose cloud services providers offering end-to-end encryption facilities. Some recommended cloud storage providers such as Sync, MEGA, Tresorit, SpiderOak, and PCloud offer end-to-end encryption options to ensure that the data stored on these companies’ servers is only accessible to the end user. These services can be used on both your computer and mobile devices. It is recommended when sharing folders and documents to others, verify and confirm the email address you share your cloud documents with. When sharing documents from your cloud storage make sure that you have the right email address.

It is recommended to create separate accounts for work and personal cloud storage, to better manage your documents and classify them according to sensitivity.

It is recommended to use a VPN when accessing your cloud storage, to hide your Internet activity and access to your cloud storage from your local Internet service provider, your Hotel Wi-Fi Administrator, or anyone who is in between you and the Internet.

Note: References to external entities and websites are only indicative and should not be considered an OHCHR’s endorsement to such entities and websites and the services provided by them. These references are provided, without warranty of any kind, either express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement. Under no circumstances shall OHCHR be liable for any loss, damage, liability or expense incurred or suffered that is claimed to have resulted from the use of these websites. The use of these websites is at the user’s sole risk. The external websites are not under the control of OHCHR, and OHCHR is not responsible for their content or any link contained in these sites.