

# 5

## Data security for physical local and external storage

Data on local storage such as your computer's hard drive (local), and on external storage devices such as external hard drives, USBs, and flash disks must also be protected and secured due to the risk of theft, seizure, or device confiscation. All information on local or external storage must be encrypted and have a copy or a backup that is stored in a remote but accessible location.



**DO**

**It is recommended to encrypt your local computer hard drive (e.g., FileVault<sup>1</sup> for Apple Computer, BitLocker<sup>2</sup> for Windows or VeraCrypt if BitLocker is not available).** Encrypting your hard drives in your local PCs can prevent unauthorized access to them, such as booting using live CDs<sup>3</sup> or simply taking your computer hard drive and plugging it into a different computer. It is common for a computer to have one physical hard drive, split into two sections, often seen as drive C, and drive D. In most cases, users use drive D to store all their data. Encrypting this logical partition (e.g., drive D) can protect your files from unauthorized access or even if the system is compromised or infected.

**It is recommended to encrypt external storage such as USB flash disks<sup>3</sup> and external hard drives using FileVault for Apple Computer, BitLocker for Windows or VeraCrypt if BitLocker is not available.** Encrypting external storage devices can allow you to store and transfer data securely through physical transfer.

**It is recommended to enable encryption during backup** (ONLY on Apple computers). Apple computer's FileVault<sup>4</sup> has a feature that

automatically encrypts your backup during the process. **Keep a copy of your external hard drive backup on the cloud – encrypted.** Keeping copies of your data from local and external storage to the cloud allows you to have an OFFSITE copy of your files.

**It is recommended to enable the hard drive password on your computer.** Hard drive password is a hardware-based password enabled in your computer firmware and it requires authentication before you can even boot your computer to Windows. However, the quality of implementation varies between manufacturers so VeraCrypt, Bitlocker or FileVault use is still recommended, regardless of using this feature or not.

**It is recommended to enable basic input/output system (BIOS) password on your firmware (Apple Computers and Windows).** BIOS is a software or a firmware that manages all the hardware in your computer. By setting up a password on it, you can block access to your computer entirely, leaving it unusable to most people because it blocks access to any bootable device.



**DON'T**

**It is not recommended to store any unencrypted sensitive information in your external storage.** Since your external storage like hard drives and USBs, are small, it is easy to lose it, or to be stolen. Keeping sensitive documents in your external storage without any encryption can put you at risk of unauthorized access or data leaks.

**It is not recommended to accept or use any external storage devices the provenance of which you do not know.** Using unknown USB or external storage may put your device at risk of infection or malware attacks. These are some of the most efficient tactics of cyber-criminals to get access to their targets. This should also apply to devices given out as gifts and/or promotions.

**It is not recommended to use external storage in transferring sensitive documents.** Unencrypted external storages are unencrypted by default. If you are to use external storage for transfer of sensitive documents, ensure that encryption is enabled on the storage.

**It is not recommended to let your external USBs and external storage lie around your workplace.** Since it is your storage device, the level of trust is high. Attackers, if given a chance may try to install something on your external storage that will run and execute once you plug it in.



**TIPS!**

### Encryption tips!

External storage: 7-Zip or VeraCrypt

Local storage (Windows hard drives): BitLocker

For Apple Computers: FileVault

**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.

<sup>1</sup> <https://support.apple.com/en-ie/HT204837>

<sup>2</sup> <https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>

<sup>3</sup> USB is an industry standard that establishes specifications for cables, connectors and protocols for connection, communication and power supply between computers, peripherals and other computers.

<sup>4</sup> FileVault is a disk encryption program in Mac OS X 10.3 and later.