Safety and Security Recommendations of Private Data

1 Encrypted information on personal computers (laptops or *desktops*)

According to the guidelines for researchers on data protection in scientific research (see point E1.d of the Guidelines), the encryption of personal data for which Iscte is responsible for processing is mandatory on personal computers. It is recommended to use some type of full protection for devices, using full encryption techniques for the information medium (disk, file system). In the case of Windows computers (Windows 10, for example), using Bitlocker and, in the case of MacOS, using FileVault. Below is some additional information for each operating system.

Windows (Bitlocker usage):

- https://carbidesecure.com/resources/how-to-encrypt-a-hard-drive-with-bitlocker-in-windows-10/
- https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10

MacOS (FileVault usage):

- https://support.apple.com/en-us/HT204837
- https://support.apple.com/en-gb/guide/deployment/dep82064ec40/web
- https://www.computerworld.com/article/3643332/how-to-use-filevault-to-protect-business-data-on-macs.html

On the other hand, we can also use tools that allow the encryption of some data (files, folders, etc.) using more common tools, such as 7-Zip (https://www.7-zip.org) or even Winzip (https://www.winzip.com). Both are tools for Windows and support the creation of compressed files with support for different types of encryption. For MacOS users, tools like BetterZip (https://betterzip.com).

2 Encrypted information on removable devices

It is also mandatory to use some type of encryption technology on removable devices, such as external disks or USB sticks. Below are some solutions for different types of operating systems.

Windows:

- Bitlocker usage
  - https://www.dummies.com/article/technology/computers/operating-systems/windows/windows-10/how-to-use-bitlocker-for-encryption-on-removable-drives-140229
  - https://www.uvm.edu/it/kb/article/encrypt-external-drive/

MacOS:

- FileVault usage

- https://www.uvm.edu/it/kb/article/encrypt-external-drive/
- https://support.apple.com/en-gb/guide/disk-utility/dskutl35612/mac

There are also a set of encryption tools that can be recommended and that work on multiple platforms.

- VeraCrypt (Windows, MacOS): https://www.veracrypt.fr/en/Home.html
- AxCrypt (Windows, MacOS): https://www.axcrypt.net/
- CipherShed (Windows, MacOS): https://www.ciphershed.org/
- DiskCryptor (Windows): https://diskcryptor.org/
- Cryptomator (Windows, MacOS): https://cryptomator.org/
- AESCrypt (Windows, MacOS): https://www.aescrypt.com/

Some of the tools listed above also support mobile operating systems such as Android and iOS, which means they can work equally well on smartphones or tablets.

Likewise, the tools mentioned above can also be used here, such as 7-Zip, Winzip or BetterZip (depending on the platform of choice).

3 VPN Transmission of private data via WWW – HTTPS and VPN

The security of the connection between the browser and the web server must always be observed, ensuring that an HTTPS connection (as opposed to HTTP) is being used. This is easily observed in the web browser, either through the URL itself or by viewing the connection properties in the browser.

Another recommendation concerns the use of a VPN, particularly when it comes to using wireless networks (Wi-Fi) in untrustworthy locations. It is recommended to use Iscte's VPN, but if this is not possible, any other VPN provider should be used. The following address offers a list of VPN providers, which can be used to make a comparison between them (most of these services are commercial, but some of them offer the possibility of limited free access):

- List of VPNs: https://www.vpnranks.com/vpn-comparison/
- Comparison of VPNs: https://www.topvpncomparison.com/

4 Secure cloud storage

The use of cloud services external to the organization is not recommended. However, if for some imperative reason it is not possible to use institutional services, it is important to select services that encrypt data in the cloud. You should always avoid placing unencrypted data in cloud services; alternatively, files must be encrypted locally on computers before being stored on cloud services.

Below are a set of secure cloud storage services that can be used as an alternative to the organization's cloud services:

- Sync: https://www.sync.com/
- pCloud: https://www.pcloud.com/
- IceDrive: https://icedrive.net/
- Mega: https://mega.io/
- iDrive: https://www.idrive.com/
- Tresorit: https://tresorit.com/
- BoxCryptor: https://www.boxcryptor.com/en/

- NordLocker: https://nordlocker.com/
- Cryptomator: https://cryptomator.org/
- Nextcloud: https://nextcloud.com/
- ProtonDrive: https://drive.protonmail.com
- SpiderOak: https://spideroak.com/
- Egnyte: https://www.egnyte.com/

Some of these services are commercial, while others are free to use.

5 Sending private information by email

Regarding sending private data via email, it is equally important to observe requirements related to their encryption. Here it is important to distinguish between webmail services and email clients that are installed on our terminal equipment.

5.1 Webmail Services

The most popular webmail services, such as Gmail.com or Outlook.com, do not offer users the possibility of encrypting the emails they send so that they can only be read by the respective recipients. There are some online webmail services that offer this type of functionality. The following list indicates some:

- ProtonMail: https://protonmail.com/
- Tutanota: https://tutanota.com/
- Mailfence: https://mailfence.com/

5.2 Email Clients

The email clients we use on our computers and mobile devices have the possibility of encrypting emails, through some mechanisms that require some type of additional configuration. The main mechanisms are S/MIME and PGP (or GPG).

5.2.1 S/MIME

S/MIME stands for Secure/Multipurpose Internet Mail Extensions and is a protocol used to digitally sign and/or encrypt emails. It is implemented in major email clients such as Microsoft Outlook, Apple Mail, Mozilla Thunderbird and many others.

Some useful links with additional information:

- What is S/MIME and how does it work?: https://kb.ptisp.com/o-que-e-como-funciona-o-s-mime/
- Installing an S/MIME Certificate and sending secure email with Outlook on Windows 10: https://www.ssl.com/pt/como/instalando-o-certificado-mime%2C-enviando-e-mail-seguro%2C-Outlook-Windows-10/
- How to install an S/MIME Certificate with Outlook on Windows 11/10: https://geekingup.org/pt- br/como-instalar-um-certificado-s-mime-no-outlook-no-windows-11-10
- Installing the S/MIME Certificate on your Mac: https://itsecurity.uiowa.edu/resources/macClientCert
- Obtaining and using an S/MIME certificate on Apple MacOS: https://www.sslmarket.co.uk/ssl/obtaining-and-using-an-s-mime-certificate-on-apple-macos/
- MacOS: Using Email Encryption in Apple's Mail: https://www.macobserver.com/tips/quick-tip/macos-using-email-encryption-apples-mail/

5.2.2 PGP (or GPG)

PGP – Pretty Good Privacy (https://www.openpgp.org/) or GPG – GNU Privacy Guard (https://gnupg.org/) are

two other examples of technologies that allow encryption of electronic mail. There are multiple PGP or GPG extensions that can be used in major email clients to allow email encryption.

In the following link you can see the list of clients and extensions, in different operating systems (Windows, MacOS) that support PGP:

- https://www.openpgp.org/software/