Liberal Democrat Data Management Encryption Guidance

Version Control

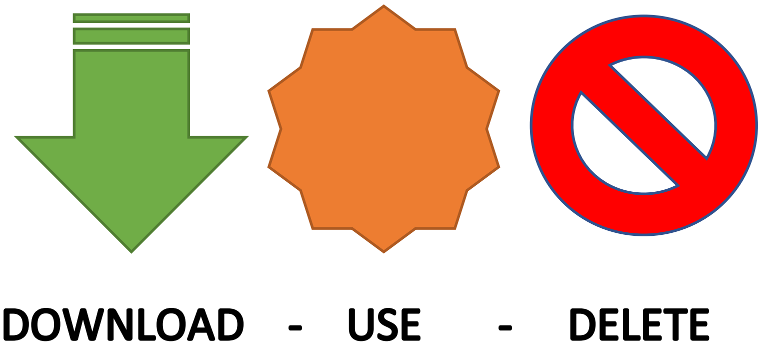
Version	Date of Issue	Author	Summary of Changes
V0.1	17/04/2018	Sanjay Samani	Initial Revision
V0.2	19/04/2018	Sanjay Samani	Added feedback from on 7 zip encryption methods.
V0.3	20/04/2018	Sanjay Samani	Clarified difference between encryption and password protection in Microsoft Office. Incorporated feedback from Working Group

Introduction

Data should be used in approved systems whenever possible [link]. These systems store data securely, data is deleted after agreed retention periods, and they support the rights of individuals under GDPR.

However, there are some times when data needs to be used, stored and shared outside of the approved systems.

Whenever possible we recommend that you Download – Use – Delete. That is download only the data you need from the approved systems. Use the data as you need. Then when you have finished, delete it.



If, however, you do need to store data outside one of the approved systems, then it needs to be encrypted.

What is Encryption and Password Protection

Data can be “password protected”. This generally means that the data is stored in a readable format, but to access it using the normal application, you need to enter a password. Howeve,r there may be other applications or methods in which you can read the data without the password.

When data is “encrypted”, the data is scrambled and unreadable by any method, unless the password is entered.

When you store or share data it must be encrypted, not just password protected.

Choosing Good Passwords

Passwords should only be used once. In particular you should not re-use a password that you have used to login to any internet accounts.

You should use a password that is a mix of numbers, lowercase letters and uppercase letters, and is at least 8 characters long.

If you use a Password Manager, for example, Last Pass, 1Passwd or Apple’s Keychain, then these tools can generate good, random passwords. This is not necessary for encrypting individual files that will be deleted after a short period of time. However, they do make it easier to create new passwords each time you need to encrypt a new file.

Sharing Passwords

If you need to share a password, you must do so via a different method from sharing the encrypted file itself. So, if you email an encrypted file as an attachment, or send the link to it, then the password must not be sent by email.

Passwords should instead be sent by text message, phone call, or a secure messaging platform, such as WhatsApp. More information on sharing data and passwords can be found in other guidance on the GDPR Guidance Page.

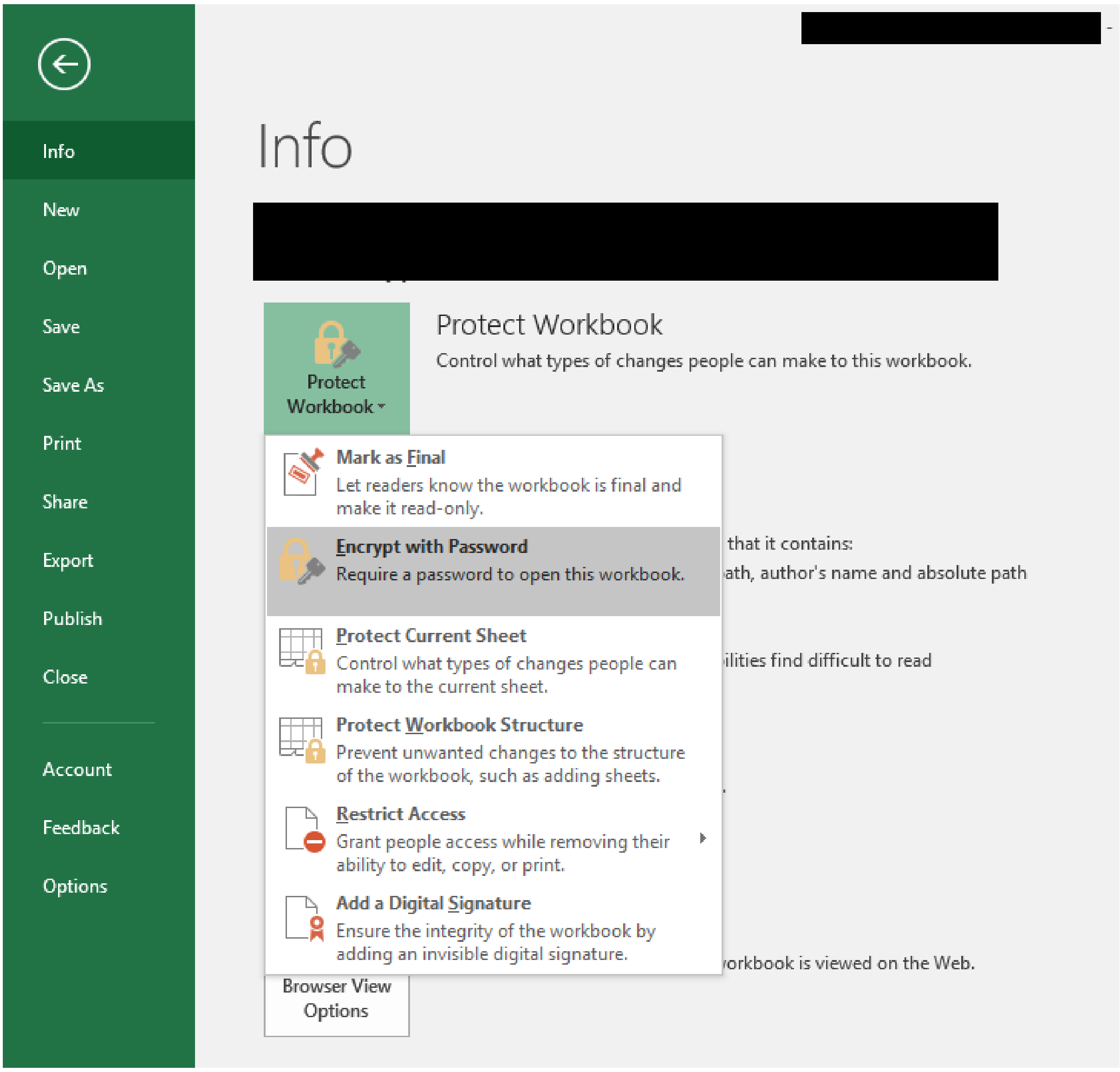
Encrypting Files

The easiest way to encrypt data is encrypting individual data files.

Encrypting Documents in Excel and Word

Microsoft Office versions since 2010 have supported encryption of individual documents. If you can download data, make use of it and then delete it, then use that method. If you need to save the data overnight, then you should encrypt it.

In Excel and Word, Select File > Info > Protect Workbook / Document > Encrypt with a Password. Enter your chosen password and save the document. If you have downloaded the file as a CSV (Comma Separated Values) or as a text file, you will need to save the document as an Excel Workbook or Word Document.



[redacted]

[redacted]

Protect Workbook

Control what types of changes people can make to this workbook.

Mark as Final
Let readers know the workbook is final and make it read-only.

Encrypt with Password
Require a password to open this workbook.

Protect Current Sheet
Control what types of changes people can make to the current sheet.

Protect Workbook Structure
Prevent unwanted changes to the structure of the workbook, such as adding sheets.

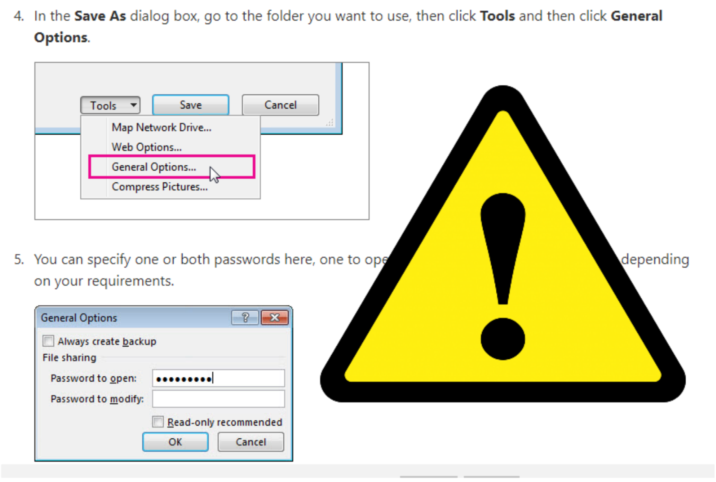
Restrict Access
Grant people access while removing their ability to edit, copy, or print.

Add a Digital Signature
Ensure the integrity of the workbook by adding an invisible digital signature.

that it contains:
ath, author's name and absolute path
ilities find difficult to read
orkbook is viewed on the Web.

Password Protection in Microsoft Office

You can also add Passwords to protect an Office Document, to restrict who can read and who can modify a document. **THIS IS NOT ENCRYPTION.** Whilst you can continue to use this feature, it must be done **in addition** to Encrypt with Password, not instead of.



4. In the **Save As** dialog box, go to the folder you want to use, then click **Tools** and then click **General Options**.

5. You can specify one or both passwords here, one to ope depending on your requirements.

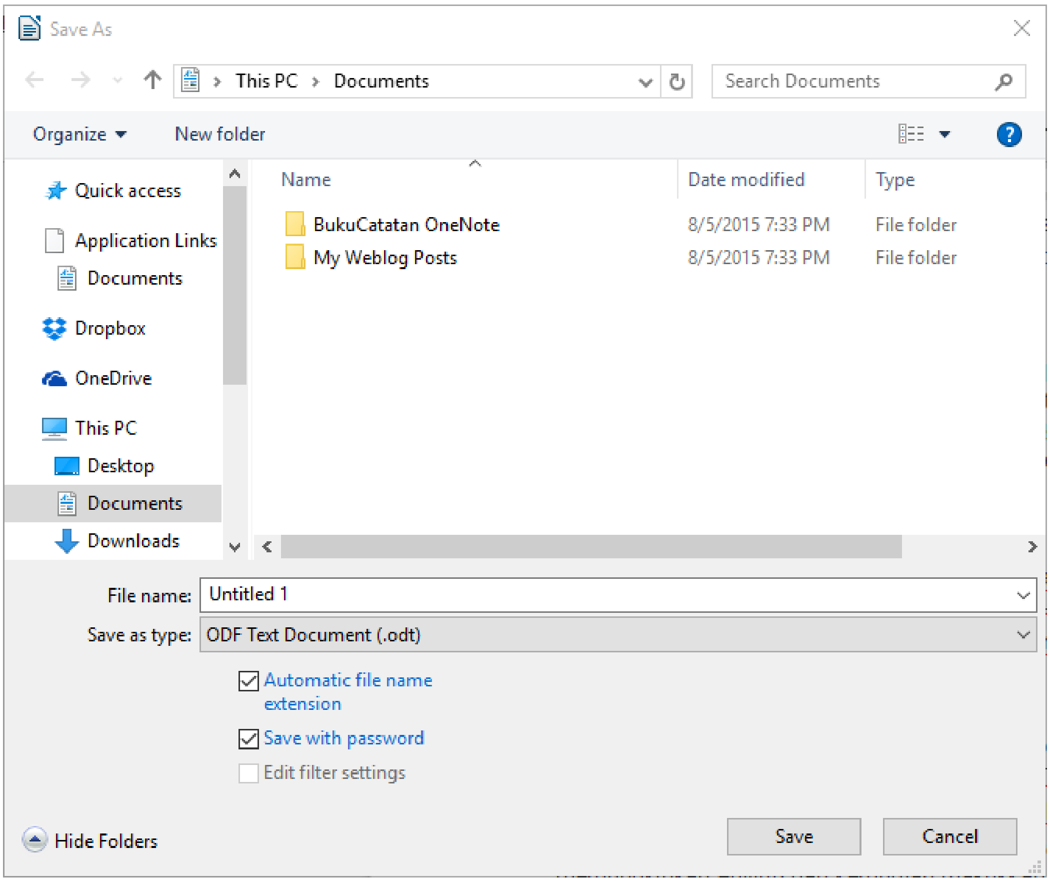
THIS IS NOT ENCRYPTION

Encrypting Documents in LibreOffice

LibreOffice is a free alternative to Microsoft Office. All documents that are saved from LibreOffice in OpenDocument format can be encrypted with a password. Documents that are saved with a password are encrypted and cannot be opened without the password.

If you can download data, make use of it and then delete it, then use that method. If you need to save the data overnight, then you should encrypt it.

To turn on protection, choose File > Save As and mark the Save with password check box. Save the document and enter your chosen password when prompted.



Name	Date modified	Type
BukuCatatan OneNote	8/5/2015 7:33 PM	File folder
My Weblog Posts	8/5/2015 7:33 PM	File folder

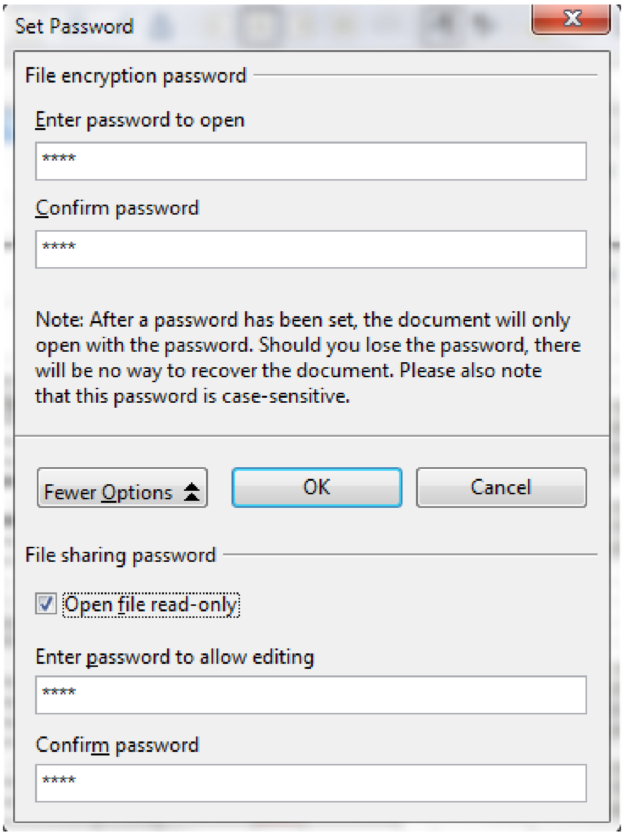
File name: Untitled 1

Save as type: ODF Text Document (.odt)

☑ Automatic file name extension

☑ Save with password

□ Edit filter settings



Set Password

File encryption password

Enter password to open

****

Confirm password

****

Note: After a password has been set, the document will only open with the password. Should you lose the password, there will be no way to recover the document. Please also note that this password is case-sensitive.

File sharing password

☑ Open file read-only

Enter password to allow editing

****

Confirm password

****

Encrypting Other Documents

Other files can also contain personal data. For example, PDFs with lists of people, photographs and media files. These also need to be encrypted. The tools for viewing and editing these do not generally have built in encryption.

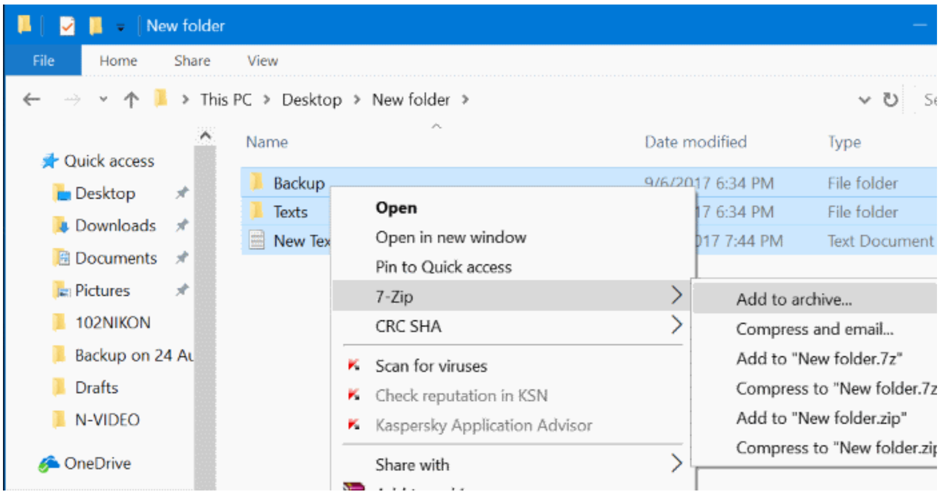
There is encryption software that will handle any sort of document, including Microsoft Office and LibreOffice documents, as well as PDFs and media files.

The recommended software below uses the same encryption for both Windows PCs and Macs, and therefore files can be shared between the two.

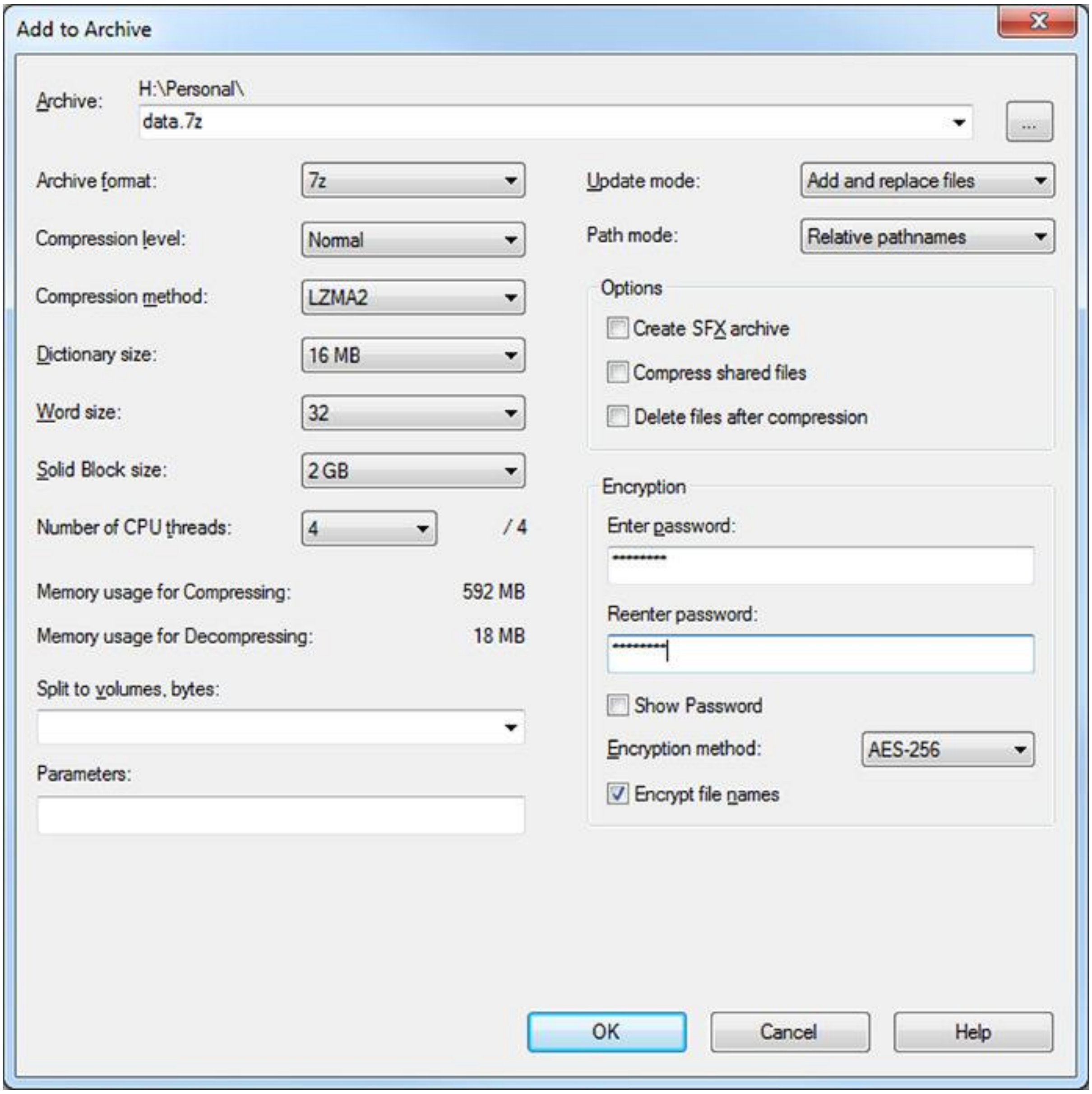
Encrypting Files on a Windows PC

The recommend software is 7-zip. Download the latest version of 7-Zip at https://www.7-zip.org/. Try the 64-bit version first as that should work unless you have an old PC. Double click on the downloaded file and follow the instructions to install.

To encrypt a file, folder or set of folders, select them in Windows Explorer. Right-click and select 7-zip > Add to archive….



In the window that appears, enter the password you have chosen in the Encryption section, and re-enter the password in the field below. Then hit OK. The 7-zip archive of the files you have selected should appear in the same folder in Windows Explorer.



Add to Archive

Archive: H:\Personal\ data.7z

Archive format: 7z

Compression level: Normal

Compression method: LZMA2

Dictionary size: 16 MB

Word size: 32

Solid Block size: 2 GB

Number of CPU threads: 4 / 4

Memory usage for Compressing: 592 MB

Memory usage for Decompressing: 18 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

Enter password: *********

Reenter password: *********

□ Show Password

Encryption method: AES-256

☑ Encrypt file names

Technical Considerations

We recommend using the “7z” Archive format with AES-256 encryption method. These are the default settings in 7-zip.

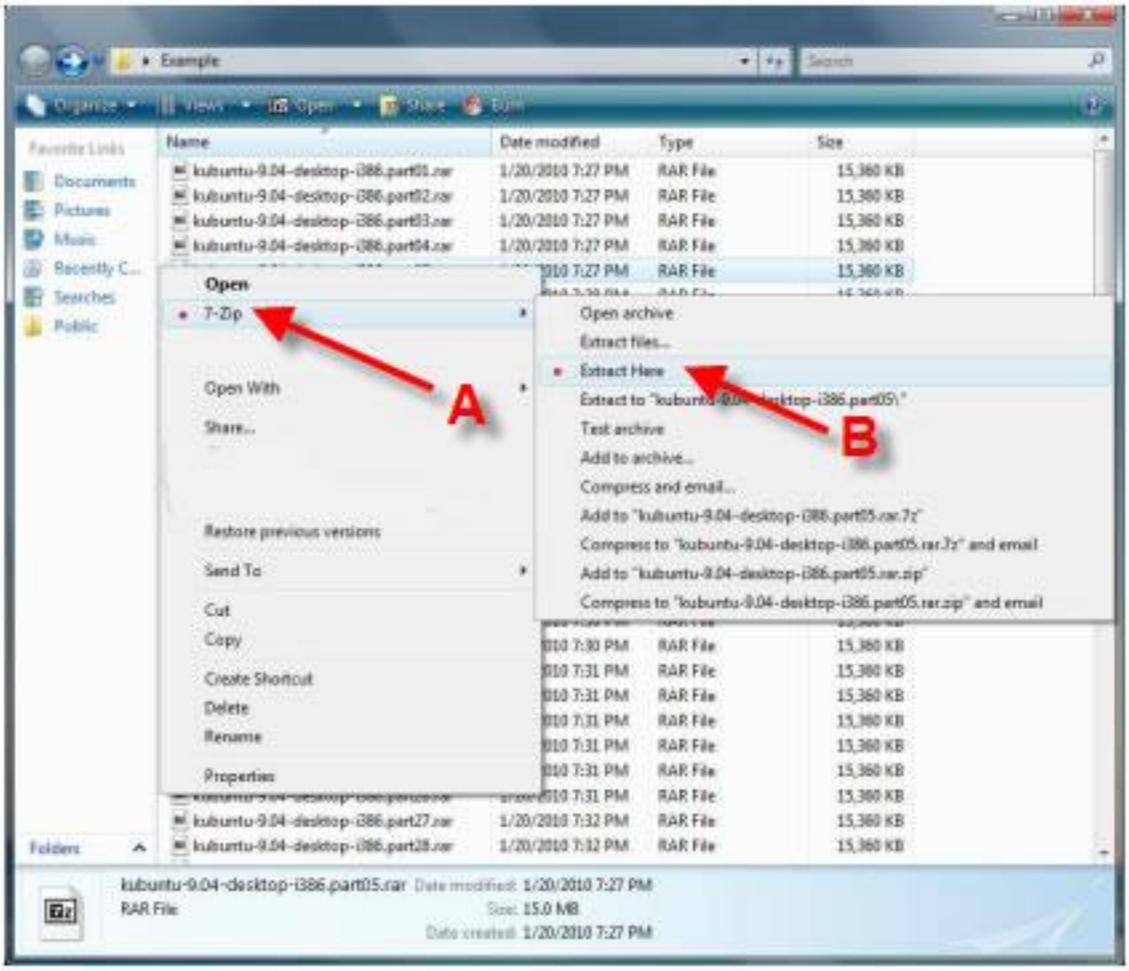
If you use the “zip” format, then the default encryption method is “ZipCrypto”. This is a weak encryption method and you are advises NOT to use it. You can use the AES-256 method with zip files, but there is no advantage in doing so. If you share a zip file with AES-256, the recipient will still need 7-zip or WinZip to open it. WinZip is a paid for product.

It is therefore easier to use the default 7z format and AES-256 encryption method. If you need to share this file, you will need to let the recipient know that they need to download 7-zip for Windows or Decompressor for Mac. See below for download links, or see the Sharing Data Guidance for more information.

Unencrypting Files on a Windows PC

The recommended software is 7-zip. Download the latest version of 7-Zip at https://www.7-zip.org/. Try the 64-bit version first as that should work unless you have an old PC. Double click on the downloaded file and follow the instructions to install.

To open an encrypted 7-zip archive, select the file in Windows Explorer. Right click on the file and select 7-Zip > Extract Here


Example
Search
Organize
Views
Open
Share
Burn
Favorite Links
Documents
Pictures
Music
Recently C...
Searches
Public
Folders
Name
Date modified
Type
Size
kubuntu-9.04-desktop-i386.part01.rar
kubuntu-9.04-desktop-i386.part02.rar
kubuntu-9.04-desktop-i386.part03.rar
kubuntu-9.04-desktop-i386.part04.rar
kubuntu-9.04-desktop-i386.part27.rar
kubuntu-9.04-desktop-i386.part28.rar
1/20/2010 7:27 PM
RAR File
15,360 KB
Open
7-Zip
Open With
Share...
Restore previous versions
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties
Open archive
Extract files...
Extract Here
Extract to "kubuntu-9.04-desktop-i386.part05\"
Test archive
Add to archive...
Compress and email...
Add to "kubuntu-9.04-desktop-i386.part05.rar.7z"
Compress to "kubuntu-9.04-desktop-i386.part05.rar.7z" and email
Add to "kubuntu-9.04-desktop-i386.part05.rar.zip"
Compress to "kubuntu-9.04-desktop-i386.part05.rar.zip" and email
A
B
kubuntu-9.04-desktop-i386.part05.rar
RAR File
Date modified: 1/20/2010 7:27 PM
Size: 15.0 MB
Date created: 1/20/2010 7:27 PM

You will be prompted for a password. Enter the password that you have been given and the files will appear in the same folder as the 7-zip file.

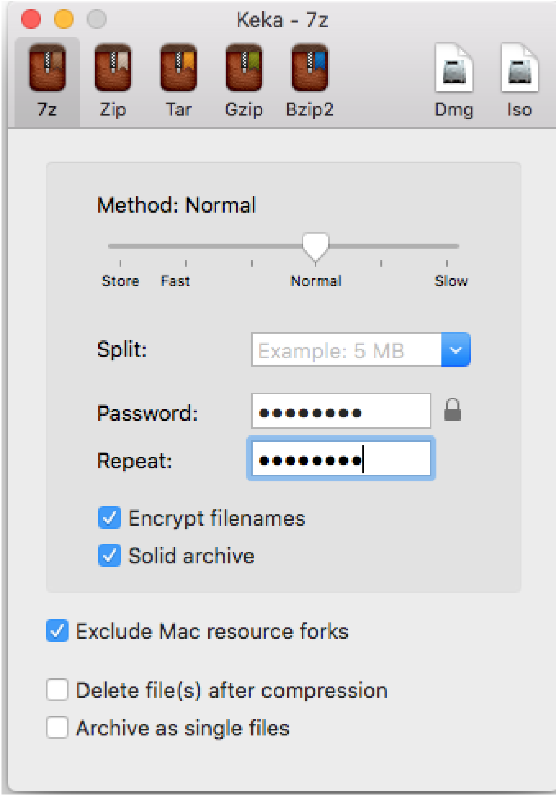
Encrypting Files on a Mac

The recommended software for encrypting files on a Mac is Keka. This has a modest cost of £1.99 at the Mac App Store. You can purchase and download Keka here: https://itunes.apple.com/gb/app/keka/id470158793?mt=12

If you do not need to encrypt files, but only open encrypted files that have been sent to you, then the recommended software is Decompressor, which is free on the Mac App Store. You can download Decompressor here: https://itunes.apple.com/gb/app/decompressor/id1033480833?mt=12

Open Keka, and use the default format, 7z. Enter the password you have chosen. Select “Exclude Mac resource forks”

Drag and drop the files you want to encrypt from Finder on to the Keka window, or application icon in the Dock.



Method: Normal

Split: Example: 5 MB

Password: ••••••••

Repeat: ••••••••

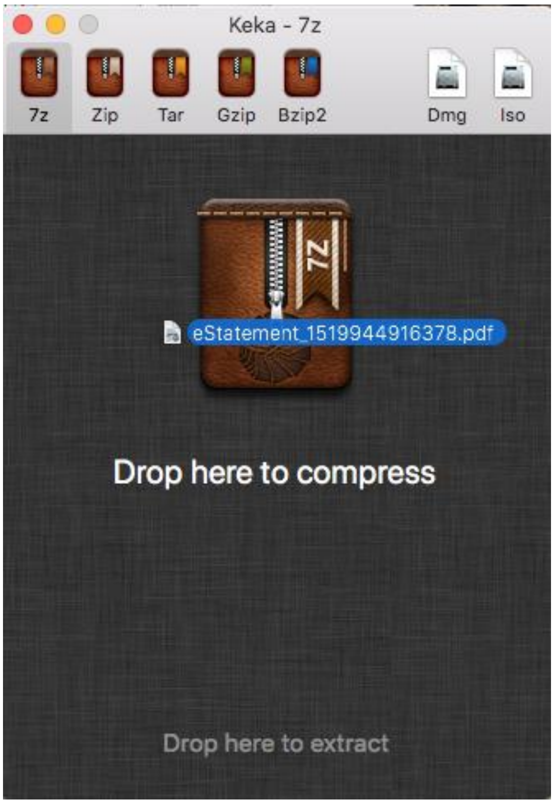
☑ Encrypt filenames

☑ Solid archive

☑ Exclude Mac resource forks

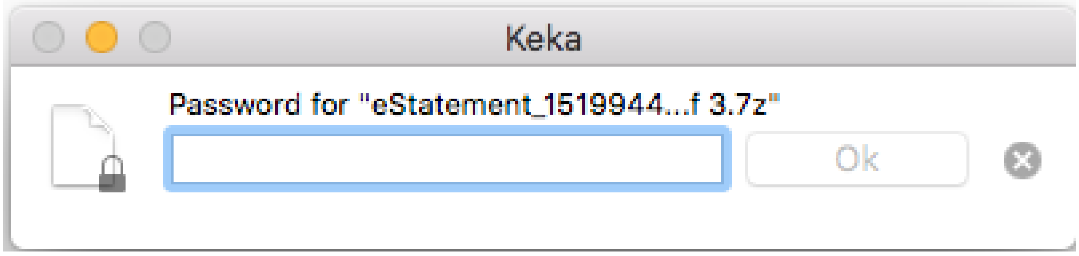
□ Delete file(s) after compression

□ Archive as single files



Unencrypting Files on a Mac

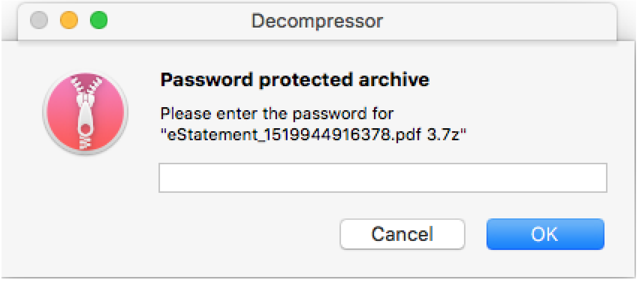
If you need to encrypt files, then you can simply use Keka as well. Double click on the archive in Finder and you will be prompted for the password:



Password for "eStatement_1519944...f 3.7z"

If you do not need to encrypt files, but only open encrypted files that have been sent to you, then the recommended software is Decompressor, which is free on the Mac App Store. You can download Decompressor here: https://itunes.apple.com/gb/app/decompressor/id1033480833?mt=12

Double click on the archive file in Finder to open it, and you will be prompted for the password.



Decompressor

Password protected archive

Please enter the password for "eStatement_1519944916378.pdf 3.7z"

Files will appear in the same folder as the encrypted archive file.

Full Disk Encryption

Again, we would recommend that you do not store data on your PC outside of the approved systems. If you need to store a lot of data on your computer, then you can encrypt the entire disk on your computer.

On a Windows PC you can use BitLocker for Full Disk Encryption. On a Mac you can use File Vault.

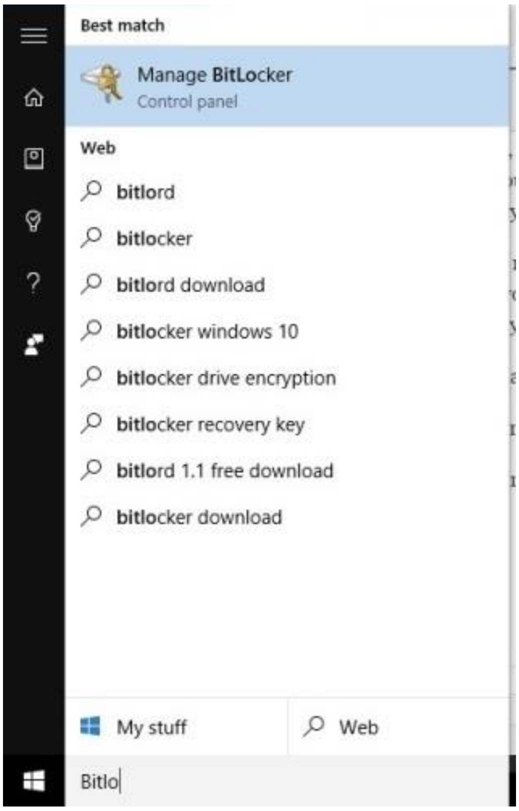
Full Disk Encryption on a Windows PC

Full Disk Encryption is not always available on Windows PCs. For the simplest method to turn it on, you will need to have a PC with Windows 10 Pro installed. The computer also needs a Trusted Platform Module (TPM), which is a special piece of hardware in the computer. If you are not using Windows 10 Pro, or do not have a TPM module, the instructions below will not work, and you will need to seek advice and support for how to add Full Disk Encryption to your Windows PC.

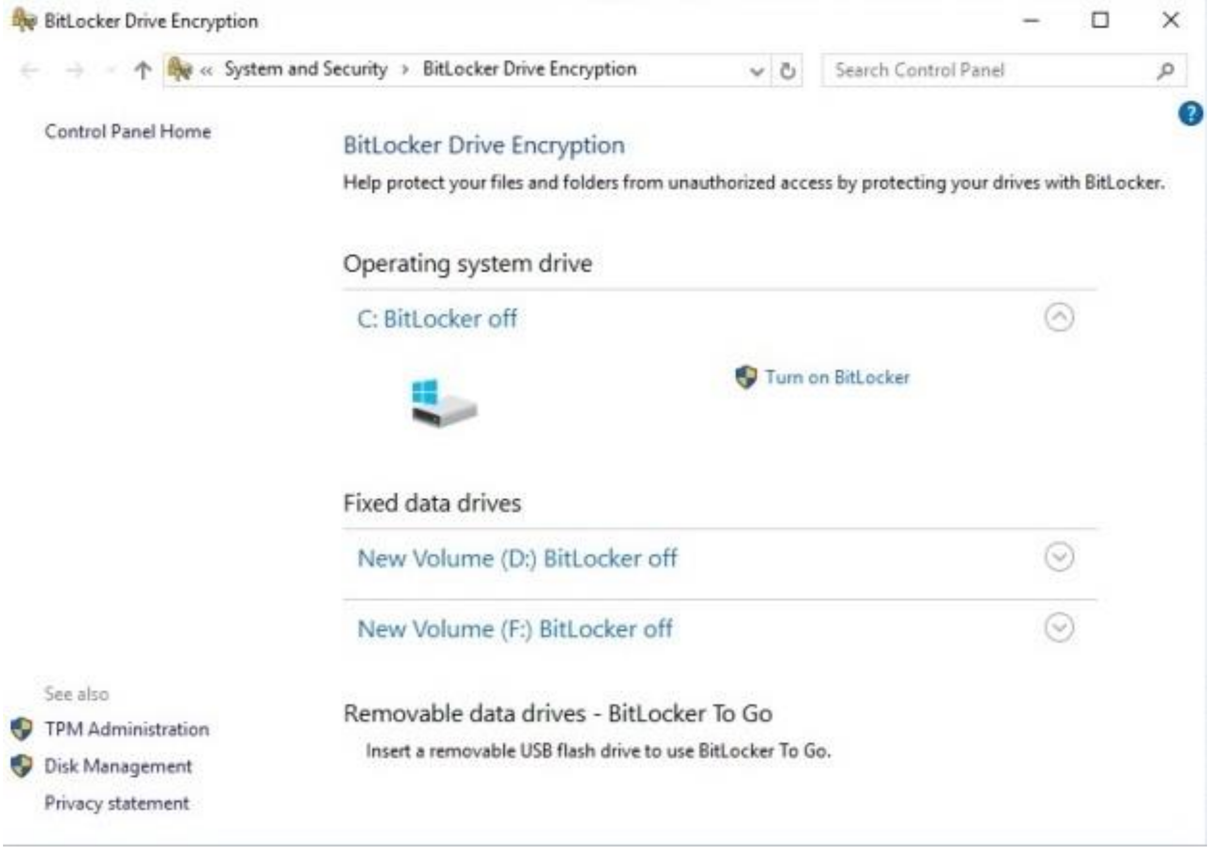
Windows 10 Pro includes software called BitLocker for encrypting your hard drive.

Go to the Start Menu (with the Windows logo in the bottom left hand corner) and type “BitLocker” in the Search field that appears.

Select Manage BitLocker that will appear in the search results. If this does not appear it may be that you do not have Windows 10 Pro.



In the BitLocker Control Panel that will appear, select “Turn On BitLocker” for the disk drive where you are going to store Lib Dem data. Normally this will be the C: Drive.


BitLocker Drive Encryption
« System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

New Volume (D:) BitLocker off

New Volume (F:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

Again, if you do not see this option, then you might not have Window 10 Pro or a Trusted Protection Module installed on your computer.

Follow the instructions and make sure that you record the Recovery Key. We recommend that you write down or print out the Recovery Key and file it in a safe place, away from where you keep your computer.

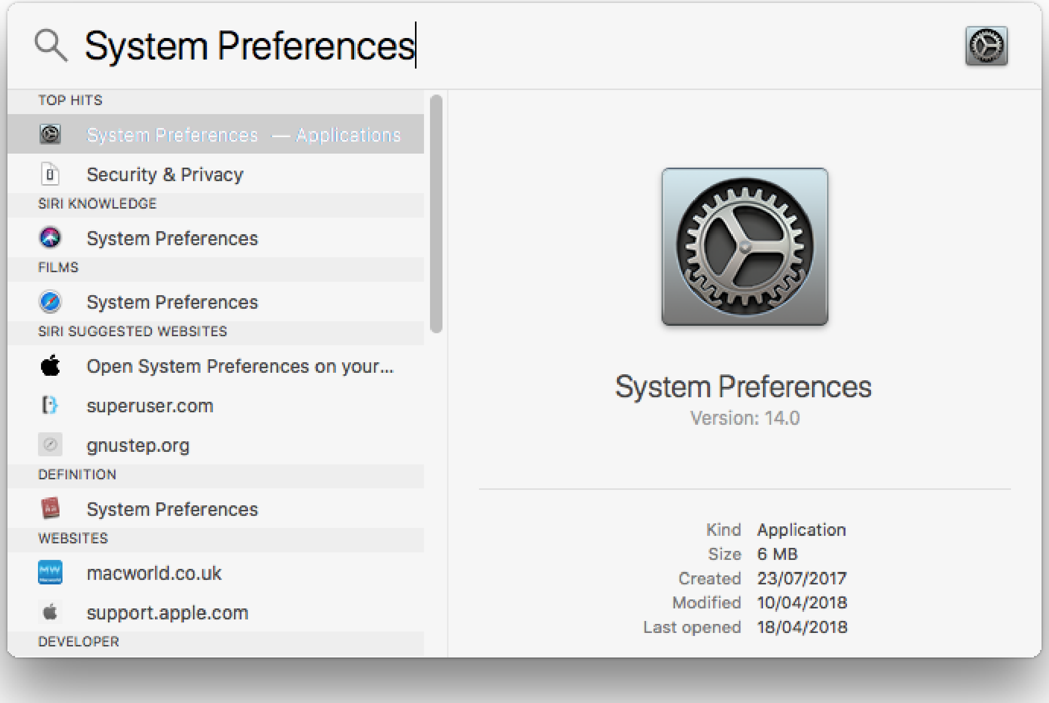
Full Disk Encryption on a Mac

Full Disk Encryption has been supported on all Macs for quite some time. Unless you have a very old Mac, these instructions should work.

Full Disk Encryption on a Mac is called File Vault and can be switched on in System Preferences.

You will need to turn on using a login and password for your Mac if you have not done so already.

Open System Preferences. This is the application with the gear icon in your Dock. Otherwise you can search for it by clicking on the search magnifying glass icon in the top right hand corner of your computer. Type "System Preferences" in the search field and open the application that appears in the search results.



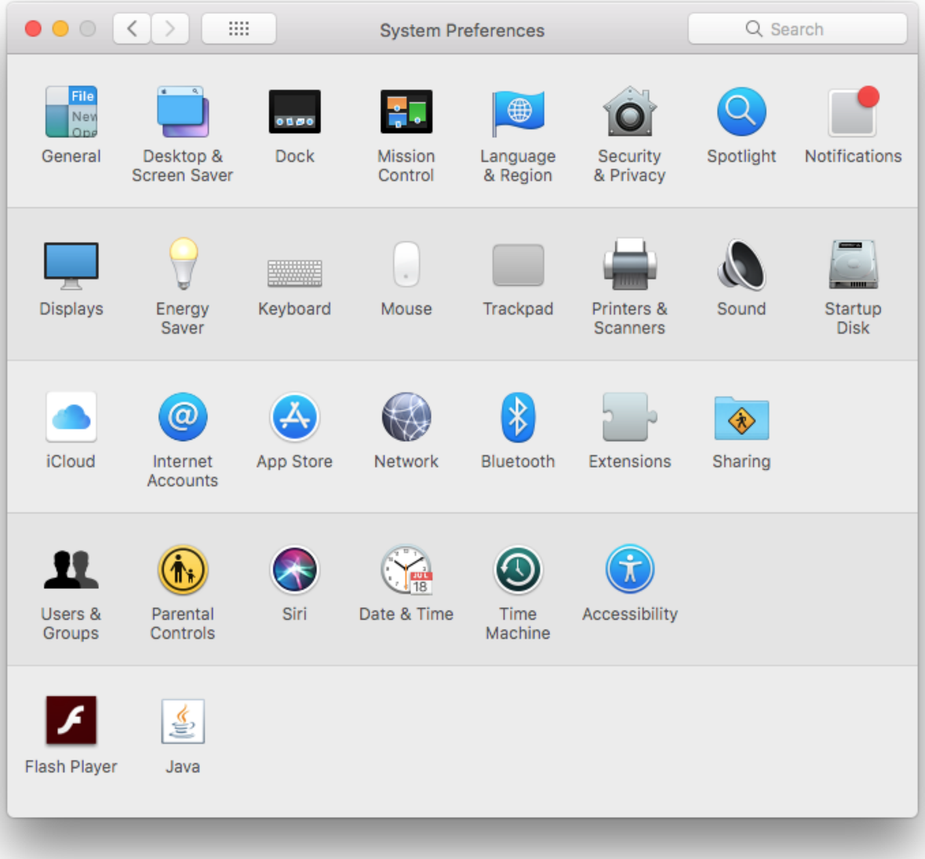
System Preferences

TOP HITS
System Preferences — Applications
Security & Privacy
SIRI KNOWLEDGE
System Preferences
FILMS
System Preferences
SIRI SUGGESTED WEBSITES
Open System Preferences on your...
superuser.com
gnustep.org
DEFINITION
System Preferences
WEBSITES
macworld.co.uk
support.apple.com
DEVELOPER

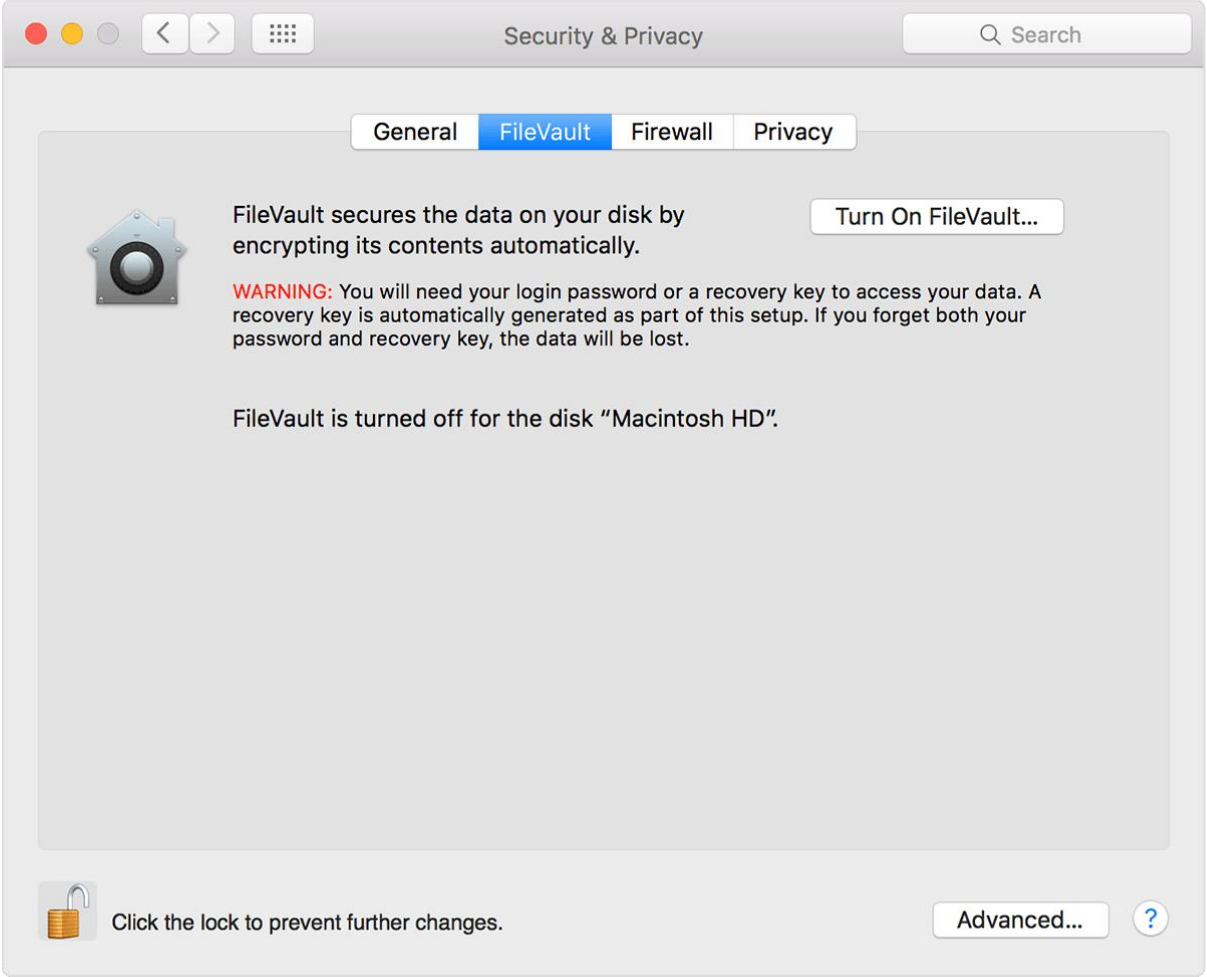
System Preferences
Version: 14.0

Kind	Application
Size	6 MB
Created	23/07/2017
Modified	10/04/2018
Last opened	18/04/2018

In System Preference, click on the "Security & Privacy" icon



Then select the “FileVault” tab and then click on the “Turn On File Vault…” button.



FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

Click the lock to prevent further changes.

Follow the instructions and make sure that you record the Recovery Key. We recommend that you write down or print out the Recovery Key and file it in a safe place, away from where you keep your computer.

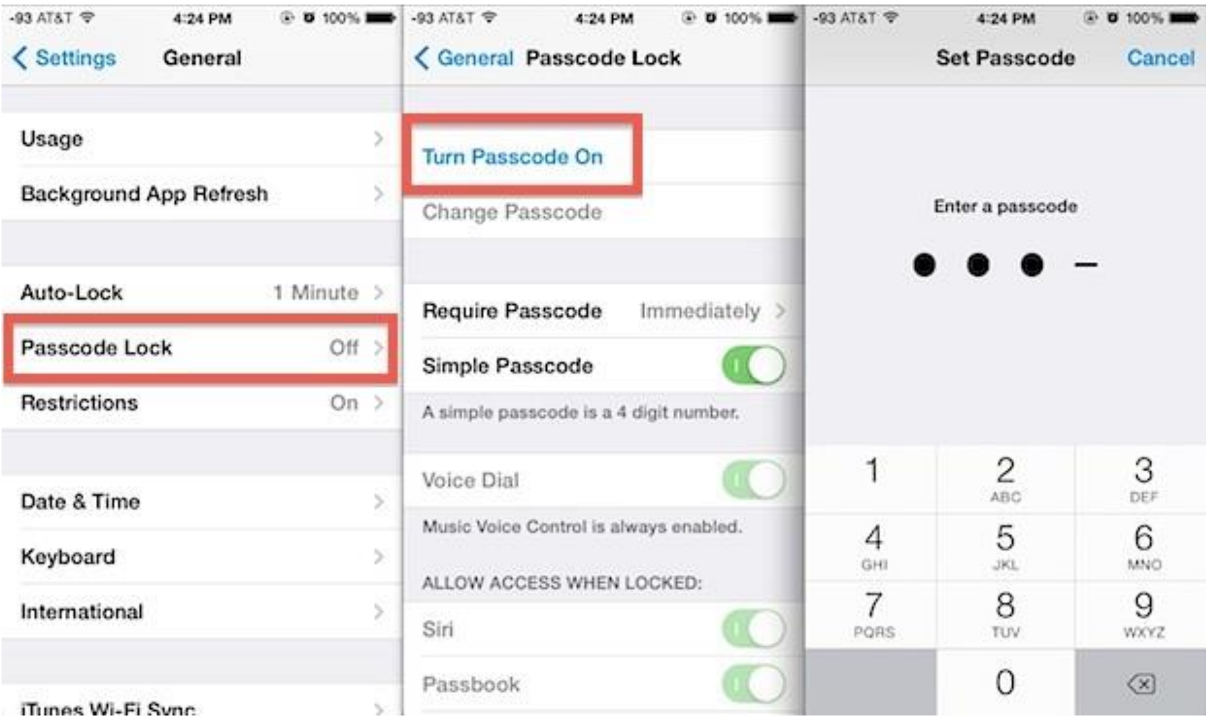
Mobile Device Encryption

You may also be storing data on your mobile devices, so we recommend they are encrypted as well. Encrypting an entire device is easier than encrypting individual files on mobile devices. Therefore, it is recommended that mobile devices, such as phones and tablets be fully encrypted.

Encrypting Apple Devices

All mobile Apple Devices, such as iPhones and iPads are fully encrypted by default. You must however turn on a passcode for the device, so that the data is not directly accessible if you lose your device.

To turn on the passcode, go to Settings > Passcode or Settings > Touch ID & Passcode and select Turn On Passcode. We recommend that you do NOT use a simple 4-digit passcode. Use either a 6-digit PIN or an alphanumeric passcode.



-93 AT&T 4:24 PM 100%

Settings General

Usage

Background App Refresh

Auto-Lock 1 Minute

Passcode Lock Off

Restrictions On

Date & Time

Keyboard

International

iTunes Wi-Fi Sync

-93 AT&T 4:24 PM 100%

General Passcode Lock

Turn Passcode On

Change Passcode

Require Passcode Immediately

Simple Passcode

A simple passcode is a 4 digit number.

Voice Dial

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

Siri

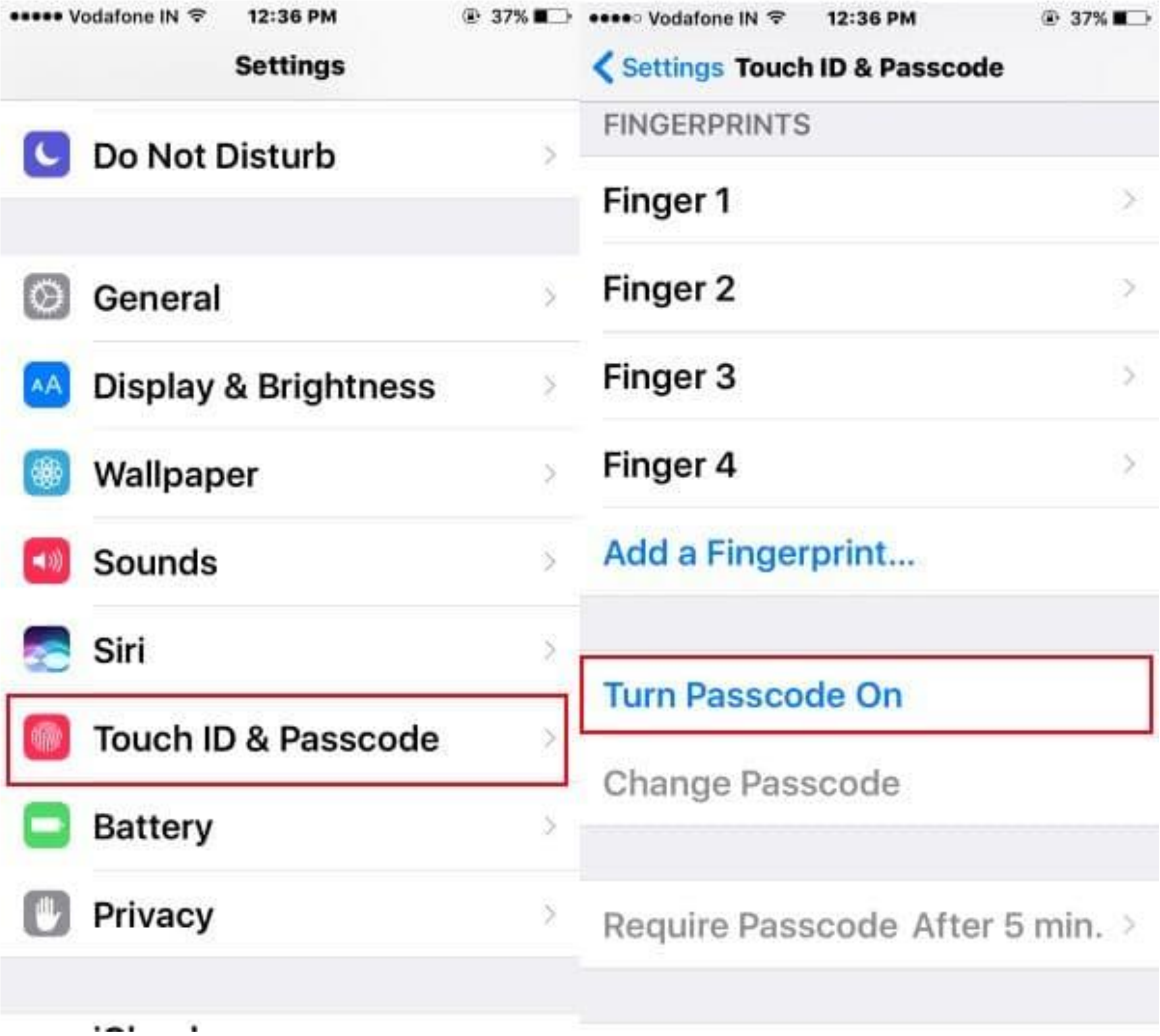
Passbook

-93 AT&T 4:24 PM 100%

Set Passcode Cancel

Enter a passcode

● ● ● –



Vodafone IN 12:36 PM 37%

Settings

Do Not Disturb

General

Display & Brightness

Wallpaper

Sounds

Siri

Touch ID & Passcode

Battery

Privacy

Vodafone IN 12:36 PM 37%

Settings Touch ID & Passcode

FINGERPRINTS

Finger 1

Finger 2

Finger 3

Finger 4

Add a Fingerprint...

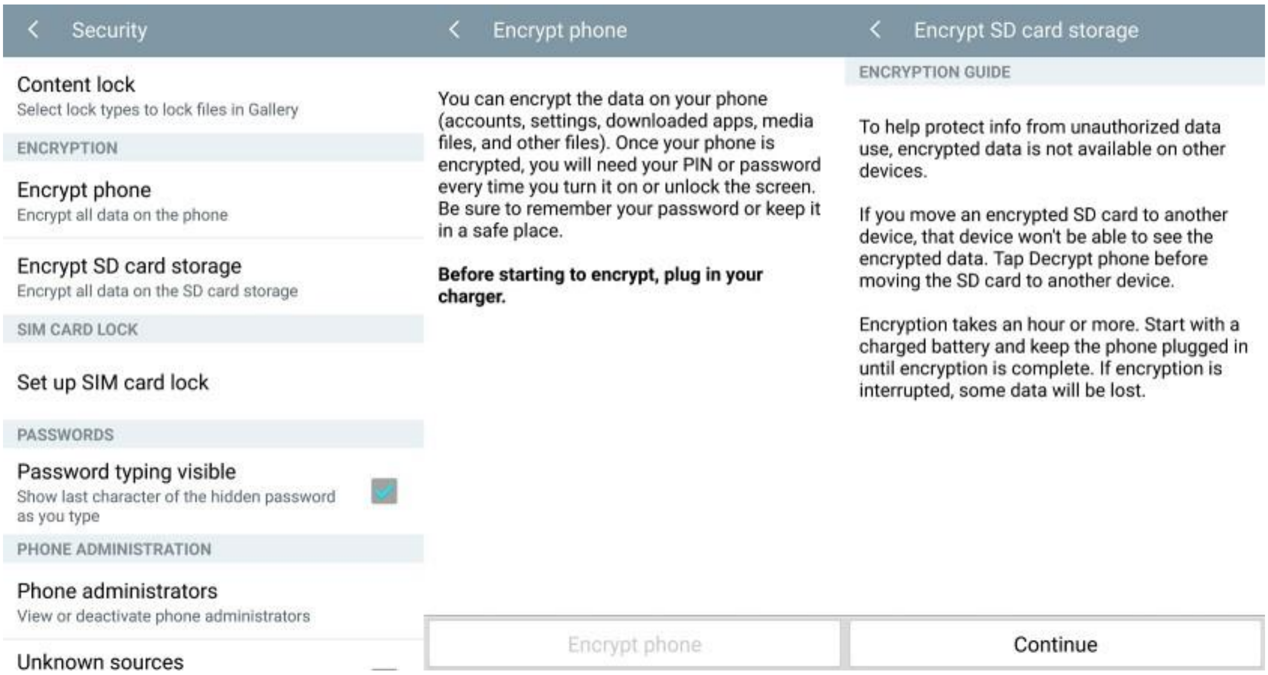
Turn Passcode On

Change Passcode

Require Passcode After 5 min.

Encrypting Android Devices

For Android mobiles and tablets running Android 5.0 Lollipop or newer, you can encrypt the device in the “Security” menu in Settings. Getting here might be slightly different depending on your phone manufacturer, but with standard Android this can be found under Settings > Personal > Security.



Security

Content lock
Select lock types to lock files in Gallery

ENCRYPTION

Encrypt phone
Encrypt all data on the phone

Encrypt SD card storage
Encrypt all data on the SD card storage

SIM CARD LOCK

Set up SIM card lock

PASSWORDS

Password typing visible ☑
Show last character of the hidden password as you type

PHONE ADMINISTRATION

Phone administrators
View or deactivate phone administrators

Unknown sources

Encrypt phone

You can encrypt the data on your phone (accounts, settings, downloaded apps, media files, and other files). Once your phone is encrypted, you will need your PIN or password every time you turn it on or unlock the screen. Be sure to remember your password or keep it in a safe place.

Before starting to encrypt, plug in your charger.

Encrypt SD card storage

ENCRYPTION GUIDE

To help protect info from unauthorized data use, encrypted data is not available on other devices.

If you move an encrypted SD card to another device, that device won't be able to see the encrypted data. Tap Decrypt phone before moving the SD card to another device.

Encryption takes an hour or more. Start with a charged battery and keep the phone plugged in until encryption is complete. If encryption is interrupted, some data will be lost.

Here you should see an option to “Encrypt phone” or “Encrypt tablet”. You’ll be asked to plug your phone in to charge while the process takes place, just to make sure that your phone doesn’t shut off and cause errors. If you haven’t done so already, you will be prompted to set a lock screen PIN or password, which you will need to enter when you turn your phone on or unlock it in order to access your newly encrypted files. Be sure to remember this PIN or password.

Android 4.4 or lower

If you’re running a handset with Android 4.4 KitKat or lower, you will have to setup a PIN or password before starting up the encryption process. Fortunately this is simple enough, head on over to Settings > Security > Screen Lock. Here you can either pick a pattern, numbered PIN, or mixed password for your lock screen. This will be the same password used after encryption, so make a note of it.

Once that’s done, you can go back to the Security menu and hit “Encrypt phone” or “Encrypt tablet.” You’ll need to have your phone plugged in and read through the warning messages, and you will almost certainly have to confirm your PIN or password one last time before the encryption process starts.