PEPPERDINE
UNIVERSITY

Guidance on the Storage of Sensitive Data

1 Scope

This document is intended to provide advice to users on the storage of sensitive data on portable devices including laptops, USB flash drives, hard drives, other portable storage devices, CDs, DVDs and other portable media.

2 What is sensitive data?

(i) *Personal data:* The Data Protection Act 1998 (DPA) defines this as "data which relates to a living individual who can be identified by that data".(1) All such data *must*be kept secure. Personal data includes, but is not limited to, student records, employee records, some research data, medical records, financial records and password information. The Information Commissioner provides technical guidance on what is considered to be personal data for the purposes of the DPA.(2)
(ii) Corporate data and intellectual property: This includes, but is not limited to, strategic planning and financial information. If you are unsure what information falls within these categories you are advised to consult your Head of Department or Division.

3 Guidelines

3.1 Only store sensitive data on portable devices or media when absolutely necessary

In nearly all cases it is not necessary and not advisable to store sensitive data on portable devices or media. However, for accessing sensitive data from a remote site we recommend that a VPN is used. Virtual Private Networks (VPNs) provide a secure remote working environment. There is also the possibility of anonymising or pseudonymising the data, so that the individuals the data relates to cannot be identified.
In circumstances in which it is necessary to store sensitive data on portable devices or media, staff should only store such data as they have an immediate need for and should remove this data when this immediate need no longer exists.

3.2 Use encryption

All sensitive data stored on portable devices or media *must* be strongly encrypted. Encrypting data will render it meaningless to anyone who does not know the key required to decrypt it, greatly reducing the risk of the data falling into the wrong hands if the device or media is stolen.

3.2.1 Considerations when using encryption

3.2.1a Length/complexity of the encryption passphrase

Encrypting and decrypting data involves the use of a secret encryption 'key', which is generated or protected by a user-supplied password or passphrase. One of the most important considerations when using encryption is to ensure that this password or passphrase is sufficiently long and complex. A passphrase is a sentence or phrase used instead of a single password and is more secure because of its length. Someone attempting to decrypt the data is not restricted in the number of attempts they can have to guess the passphrase, so it is essential to make the passphrase complex enough that the amount of time it would take to guess it makes this impractical.

The following recommendations for choosing passphrases apply:

- The longer the better
- Use a mixture of lowercase, uppercase, numbers and symbols
- Avoid single dictionary words (long phrases using multiple dictionary words are generally ok)

It is essential that the passphrase is kept secret. When choosing a passphrase, choose one that you will remember and avoid writing it down. Bear in mind that if you forget your passphrase you will not be able to access the encrypted files. If you really need to write it down somewhere, do so in a way that it is not obvious what it is for and do not keep this with the portable device or media. Also be aware of the provision under the Regulation of Investigatory Powers Act (2000) for public authorities to demand the disclosure of encryption keys.(3)

3.2.1b Backups

When encrypting data for storage on portable devices or media, ensure that an unencrypted backup of the data exists in a secure environment. This will protect against loss of the data if the device is lost or damaged, if you forget the encryption key, or if the encryption software fails.

3.2.1c Power Management on laptops

Recent research shows that it is possible for an attacker to retrieve encryption keys from a computer's memory while it is switched on or shortly it is switched off. When using power saving modes such as standby, sleep or hibernate, the contents of memory are preserved and therefore a laptop stolen in one of these states may be vulnerable to this kind of attack. Therefore it is recommended that laptops using encryption are completely shut down before being transported or left unattended.

3.3 Encryption Software

There are a large number of encryption packages available. The packages below are given as suggestions only, on the basis that they are either free or built into the operating systems.

3.3.1 On-the-fly encryption software

Packages which perform 'on-the-fly' encryption make the encryption transparent to the user, by automatically encrypting files when they are saved to an encrypted drive or volume. The user will usually be required to type their encryption passphrase either when the computer is started or when the encrypted volume is mounted.
The following on-the-fly encryption packages are suggested for use:

3.3.1a Windows

BitLocker

BitLocker is built into current versions of Windows (7, 8 and 10) and encrypts whole volumes (including the system partition), both fixed and removable drives. BitLocker works by encrypting the entire Windows operating system drive on the hard disk and checking the integrity of early boot components and boot configuration data on computers that have a Trusted Platform Module (TPM) version 1.2.
BitLocker is only available in the Enterprise and Ultimate editions of Windows.
Please see the Microsoft web site for more information:

- BitLocker Drive Encryption in Windows 7: Frequently Asked Questions
- BitLocker Drive Encryption Step-by-Step Guide for Windows 7
- BitLocker Overview - Windows Server 2012, Windows 8
- BitLocker - Windows 10

3.3.1b Mac OS X

FileVault

FileVault is built into OS X by default. FileVault encrypts the user's home directory and all the files in it. Only the user's login password can decrypt and mount this drive image, so at login the home directory becomes available as usual - its icon, however, looks like a lock. After the initial startup, only users enabled in FileVault can log in; other users need an administrator to log in first.
Please see the Apple web site for more information: OS X El Capitan: Encrypt the contents of your Mac with FileVault

3.3.1c Linux

dm-crypt

dm-crypt is fully integrated into the Linux kernel and provides transparent encryption. It supports encrypting whole disks, partitions, logical volumes, as well as files, and can be used with any file system.

3.3.2 Encrypted compressed archives

An alternative to the 'on the fly' encryption software mentioned above, is software that will create an encrypted compressed archive of your files. These are generally not as convenient to use as 'on the fly' encryption as they are not transparent to the user. You cannot just save a file to an existing encrypted archive, instead you would have to unencrypt the archive and then encrypt all the files again.

There are some advantages of encrypted archives that make them worth mentioning. One is that the files are compressed as well as encrypted, so they take up less space and are therefore useful for making off site backups of important data. Another is the fact that the software is already commonly used for creating compressed archives.

Encrypted archives are also more suitable for emailing. When emailing encrypted files, it is important that care is taken when exchanging the encryption passphrase. This should be done over a medium other than email and must *never* be mailed with the encrypted file.

Examples include:

WinZip - the most well known archiver (use version 9 or later) - www.winzip.com

7Zip - a free, open source equivalent - www.7-zip.org

If these type of products are used for encryption it is essential that a sufficiently strong encryption algorithm is used. WinZip before version 9 and early clones supported only "WinZip encryption" (sometimes known as Zip 2.0 encryption or ZipCrypto) which is insufficient and passwords of any strength can easily be recovered.

AES encryption can be considered sufficiently strong. The latest versions of the packages mentioned support AES. Given the choice of 128, 192 or 256 bit AES you might as well choose the strongest, 256 bit, although 128 bit AES is by no means weak. If your archiving software does not mention AES when encrypting files, it probably uses the weak Zip 2.0 encryption and *must not* be used.

3.3.3 Forms of encryption to avoid

The forms of encryption listed below should be avoided as the passwords can easily be broken:

Zip 2.0 encryption (as mentioned above)

References

(1) http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

(2)http://www.ico.gov.uk/upload/documents/determining_what_is_personal_data/whatispersonaldata2.htm

ICO Guidance re: Personal and Sensitive Data can be found at:https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

(3) http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/