London School of Economics & Political Science

Information Management and Technology

Guidelines

Encryption Guidelines

Jethro Perkins
Information Security Manager

Summary	Guidelines for appropriate use of encryption and suggested encryption tools
Version	Release 1.2
Date	29 May 2014
Library reference	IMT-GD-102

Table of contents

1 Introduction

1.1 What is encryption?

Encryption is a way of encoding information so that it cannot be read without the appropriate key to decode it. It is a way of rendering files, volumes or hard disks extremely secure.

1.2 When should encryption be used?

Encryption should be used to secure data that are in transit or else are accessed and held outside LSE systems, for instance on a home workstation, or on devices that are easy to steal or lose (such as laptops, tablets etc).

1.3 What should be encrypted?

Not all LSE data are so valuable that they need to be encrypted.

Encryption should be used when you are dealing with data (including the Data Protection Act's definition of *Sensitive Personal Data*) which the LSE would classify as 'Confidential'.

The accidental or deliberate loss of 'Confidential' information could cause LSE reputational damage, lead to fines being levied by the Information Commissioner's Office, and result in the cancellation of, or failure to win, research contracts.

1.4 Evaluating what data are Confidential

You can read about LSE's Information Classification scheme here.

Confidential information would include identifiable records of someone's racial/ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health condition, details of their sexual life or their criminal record.

Other examples include salary information, individuals' bank details, passwords, large aggregates (>1000 records) of personally identifiable information including name, address, telephone number, HR system data.

If you are only dealing with Confidential data that is not being removed from LSE systems, is not being emailed or otherwise transmitted, but is being accessed and processed entirely by a machine onsite or hosted in an LSE datacentre (e.g. through a remote desktop connection), you do not need to use encryption for data unless it is contractually mandated. You should, however, make sure that the connection you are using to talk to LSE systems is encrypted (e.g. you are using a VPN connection, or an https web connection. Please talk to the IT Service Desk if you are not sure.)

Any contractual obligations attached to the data (e.g. as stipulated in a research contract) take precedence over these guidelines.

It is up to you to assess the data that you're using and take responsibility for the measures you use to protect them. If you need further guidance or help, please contact the IT Service Desk

2 Guidelines

2.1 Using Confidential data off-site

2.1.1 PC / Mac:

If you are working with 'Confidential' data off-site on a PC / Mac workstation or laptop, please make sure that the machine requires an explicit username / password to log on, and that the hard drive and any attached external hard drives or other removable devices that will store 'Confidential' data are encrypted. See the *Remote Access and Mobile Working Guidelines* for further information.

2.1.2 External Hard Drives / Removable Devices

There are a range of options for using encryption on removable devices.

If you are going to put 'Confidential' data on removable devices, either the data **or** the device should be encrypted.

You can purchase hardware-encrypted external hard drives and flash drives should you need to store large amounts of 'Confidential' data off-site.

You can also create encrypted volumes on external hard drives or removable devices, or create encrypted zip archives or individually encrypted files on removable devices.

2.1.3 Tablet / Phone

If you are using a tablet or a phone to access these data, we recommend that you make sure that the phone's storage is encrypted (which has to be performed actively on an Android phone or tablet) and that usage requires the entry of a passphrase (not just a 4-digit PIN). The passphrase is effectively the key to the encryption, so a simple PIN only provides very weak encryption that is easily cracked.

2.1.4 Individual Files / Attachments

If you are emailing attachments containing 'Confidential' data we recommend that the attachments are encrypted. Remember that emails are like postcards: easily intercepted and read, and also easily passed on to a further recipient. It is not a wise idea to include 'Confidential' data in the body of an email or in unencrypted attachments. The best practice is to distribute the passphrase to the encrypted attachment in a separate email.

An alternative to full disk encryption for storing 'Confidential' data off-site is to encrypt each file individually. This may be the best option if you only have a small amount of Confidential data to work with. It is, however, impractical for large volumes of data.

2.2 Encryption Standards – what to use

There are many different encryption algorithms available. The accepted standard to use wherever possible is called **AES 256-bit**. However, not all encryption programs support this, so under most circumstances, unless contractually stipulated, AES 128-bit, 3DES, or Blowfish, when combined with a complex passphrase, provide an adequate level of protection.

If you're in any doubt, please talk to the IT Service Desk.

3 Easily available encryption software

3.1 Encrypting volumes and disks

3.1.1 PC

Enterprise and Premium and Pro editions of Windows Vista, 7 and 8 come with BitLocker as standard, which you can use to encrypt drives, disks and usb sticks. For other editions, you can purchase drive encryption e.g. from Symantec: http://buy.symantec.com/estore/clp/productdetails/pk/drive-encryption

3.1.2 Macs

Mac OS X 10.7 (Lion) and more recent releases have FileVault functionality built in that can be enabled to encrypt the hard disk. See http://support.apple.com/kb/HT4790 for more information.

3.1.3 Linux

Linux

Most versions of Linux come with built-in options for configuring Full Disk Encryption (FDE)

3.1.4 iPhones and iPads

Volume encryption is enabled by default on iPhones and iPads if PIN or passphrase access is configured. As the strength of the encryption is dependent upon the complexity of the PIN or passphrase, it is, however, meaningless unless you have a passphrase rather than just a 4 number PIN. To change from a simple passcode to a passphrase, go to Settings – General – Passcode Lock – Switch off 'Simple Passcode'.

3.1.5 Android Devices

Storage volume encryption is available as an option you can enable on Android devices. See http://support.google.com/android/bin/answer.py?hl=en&answer=1663755 for more details.

3.2 Encrypting individual files for use on a PC

3.2.1 Axcrypt

Axcrypt (http://www.axantum.com/axcrypt/Downloads.html) is intuitive and user friendly, but is limited to 128-bit AES encryption, and the files it creates cannot be opened on a Mac.

3.2.2 7zip

7zip (http://www.7-zip.org/) is less user-friendly but can create zipped archives with 256-bit AES encryption, that can also be opened using the unzip function on Macs. You can find instructions of how to zip and encrypt using 7zip here: http://www.medicalnerds.com/how-to-encrypt-zip-files-securely-using-7zip/.

3.3 Encrypting individual files for use on a PC or Mac

3.3.1 7zip

As mentioned above 7zip can create encrypted zipped archives that can be opened on PCs or Macs. Encrypted zip files created on a Mac should be able to be opened on a PC using 7zip. Instructions on zipping on a Mac are available here: http://operating-systems.wonderhowto.com/how-to/create-encrypted-zip-archive-mac-os-x-and-windows-0139565/. There are also 7-zip variants available for Macs which you can find here: http://www.7-zip.org/download.html

3.3.2 MEO Encryption

MEO Encryption Software (http://www.nchsoftware.com/encrypt/index.html). This has a common interface for both Mac and PC users, and therefore is more user friendly than either 7zip or the Mac zip file encryption, but uses an older encryption algorithm: 3DES.

4 Other Issues

4.1 Encryption keys

The key to all encryption is the passphrase that is used to decrypt a file of volume. This is known as the encryption key. Losing or forgetting your encryption key will render your encrypted files or device unusable.

It is therefore advisable to keep a copy of your encryption key somewhere safe (and preferably without a reference to what it opens).

Some encryption software, such as BitLocker, offers the ability to create a recovery disk in case the encryption key is lost. IMT can store this disk for you in a locked fireproof safe.

4.2 Countries which may request you hand over the key to any encrypted volume

The border agencies and police forces of some countries are extremely unhappy with the presence of encrypted files or volumes that they cannot decrypt. Government agencies in *any* country may demand you hand over the encryption keys or otherwise demonstrate what is contained within an encrypted folder. This may happen with or without any legal enforcement in place to encourage such a situation.

If you are travelling abroad with encrypted Confidential data this creates the risk that such data may be exposed to unintended recipients, breaching the Data Protection Act.

If the encryption software you are using is not a mass market product freely available to the public, you may need to obtain a Cryptography Open General Export Licence (OGEL) before travelling abroad with it. This will not be the case if you are using any of the products included in these *Encryption Guidelines*. See the UK Government's note on the export of Cryptographic items at https://www.gov.uk/export-of-cryptographic-items and for more information about OGEL rules https://www.gov.uk/dual-use-open-general-export-licences-explained.

4.2.1 The Wassenaar Arrangement

In theory, any citizen of a member country of the "Wassenaar Arrangement" may travel to any of the other countries who have signed the agreement with an encrypted device, under a "personal use exemption," which holds as long as that person does not create, enhance, share, sell or otherwise distribute the encryption technology whilst visiting.

Russia and Ukraine, whilst being signatories of the Wassenaar Arrangement, do not permit "personal use exemptions."

A list of Wassenaar Arrangement countries can be found here:
http://www.wassenaar.org/participants/index.html

Please note that a "personal use exemption" does not guarantee that a citizen of these countries will not be requested to hand over encryption keys.

4.3 Policy Awareness and Disciplinary Procedures

The loss or breach of confidentiality of personal data is an infringement of the Data Protection Act 1998 and may result in criminal or civil action against LSE. The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against LSE. Therefore it is crucial that all users of the School's information systems adhere to the Information Security Policy and its supporting policies as well as the Information Classification Standard.

Any security breach will be handled in accordance with all relevant School policies, including the *Conditions of Use of IT Facilities at the LSE*.

4.4 Further Policies, Codes of Practice, Procedures and Guidelines

These guidelines sit beneath LSE's overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce these guidelines. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

The below list of current policies is in no way authoritative and new policies will be published on the LSE website as they become available.

Associated polices:

Conditions of Use of IT Facilities at LSE
Policy on the use of mobile telephony equipment
Policy on the use of school-funded iPhones
Conditions of use of the residences network
Password Policy
Asset Management Policy
Data Protection Policy

Standards and Guidelines:

Information Classification Standard
Remote Access and Mobile Working Guidelines
Guidelines on the use of Cloud storage

4.5 Review and Development

These guidelines shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the Information Security Advisory Board (ISAB) and an auditor external to IT Services as appropriate.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.