THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Technical

Data Encryption requirements for end users

1. Introduction

1.1 Purpose

The use of encryption is becoming more widespread under heightened requirements for security among data suppliers, regulators and end users.
This policy standardises and regulates the use of encryption by users at LSE.

1.2 Scope

Ad hoc use of encryption products by members of the LSE Community for the encryption of confidential data, where LSE is the data controller or the data processor.

It includes:

- Encrypting files with the intention of transporting them securely
- Encrypting files or folders to secure internal data (above and beyond the restrictions provided by folder level user permissions)
- Holding sensitive data on cloud storage that is not run or centrally managed by LSE (for example Dropbox)
- Encryption of storage volumes, or computer hard drives
- Ad hoc or non-centralised backups

1.3 Out of Scope

- The routine processing of data in corporate systems, for example as used by HR or ARD.
- Corporately commissioned Cloud systems, which will be evaluated before contracts are signed.
- Data LSE defines as Public, Internal or Restricted.
- Data you access remotely, but which is still opened, processed and hosted on LSE systems (e.g. you're using the remote desktop, or editing data online in SharePoint)

2. Policy

2.1 Encryption requirements

The use of encryption by users may be mandated by the following:

- Data supplier requirements
  - This could be required as part of a contract to get research data
  - It could be part of contractual requirements where we are required to generate data
- You're taking personal data outside the LSE, for example
  - A spreadsheet containing personal data (such as salaries) on a laptop at home
- LSE's Information Security Policy and Information Classification Standard (for example, having to email personal data in a spreadsheet, or storing recorded interviews on mobile devices)
- LSE's Laptop Encryption Policy
- Backups (all LSE corporate backups are encrypted – user backups should be too)

It may also be something people choose to use, even though it isn't mandated – for instance, LSE-hosted spreadsheets containing salary data, or exam questions.

2.1.1. When must I encrypt data?

- You must encrypt confidential data whenever you remove it from LSE systems. So, for example:
  - You need to email a sensitive spreadsheet to a supplier
  - You need to protect recorded interviews that have been conducted in the field
  - You're sharing a sensitive dataset via Dropbox with a collaborator from another university
  - You're conducting sensitive fieldwork that, due to bad Internet access, will have to be stored on a local laptop.

2.1.2. When don't I need to encrypt data?

- If it's not confidential (i.e.it doesn't contain personal information or embargoed data) you don't need to encrypt it
- If it's confidential but staying within LSE systems (e.g. H: space, S: drive, SharePoint, OneDrive) you don't need to encrypt it – the access controls around those systems should appropriately control who can see it, although it never hurts to check that only the appropriate people have access
- This means that confidential information that you remotely access via the LSE remote desktop does not have to be encrypted (unless a data supplier expressly requires it) – it's not being held on your device.

2.1.3. How do I encrypt data?

- Files
  - Encrypting files is good for when you need to send individual files, either over email, or via Dropbox, or on USB sticks etc.

    - If you need to encrypt an *individual* Microsoft Office document, you can do so via 'File' – 'Info' – 'Protect Document' – 'Encrypt with Password'.
    - Other documents can be encrypted using 7zip, which is on all LSE managed desktops, and can be freely downloaded. It works across different operating systems. 7zip can encrypt multiple files in one archive.
        - LSE has a guide to using 7zip
    - Remember the encryption is only as good as the password you set. Make sure:
        - the password at least meets LSE's Password Policy (8 characters, one uppercase, one lowercase)
        - the password is transmitted to anyone else who may need it by a different method to the delivery of the file: e.g. use a text message, or a phone call
- Folders, Volumes
    - Windows folders can be encrypted using the 'Encrypt contents' option. This, however, limits the use of the folder only to the person who encrypted it, using only the computer the encryption was created from. It will not be backed up automatically, so use with extreme caution
    - Free encryption tool VeraCrypt can be used to create encrypted volumes. These can be shared by anyone who has access to where the volume is stored, and who knows the volume password.
    - Veracrypt volumes can also be created inside Dropboxes and OneDrives.
- Devices and drives
    - Hard drive encryption and device encryption, when combined with a complex password or device PIN, is considered an adequate protection by the ICO against data breaches generated by lost or stolen devices
    - LSE laptops from December 2017+ are encrypted by default
    - Older ones may not be. If you're going to be storing confidential data on a laptop, it can be retroactively encrypted for you – contact the IT Service Desk
    - Most Windows devices can be encrypted using BitLocker
    - Most Macs can be encrypted using FileVault
    - If you have neither of these options, you can still use VeraCrypt – contact the IT Service Desk
    - iPhones and iPads are automatically encrypted
    - Encryption is an option that needs to be switched on with most Android devices
- USB and mass storage devices
    - BitLocker, FileVault and VeraCrypt can all be used to encrypt USB and other mass storage devices
    - Many mass storage devices ship with hardware encryption
    - If confidential data will be stored on detachable mass storage devices, the device or the data *must* be encrypted

2.2 Encryption Standards

Where encryption is required:

- Files, folders, volumes and drives will be encrypted by default to AES-256
- Hardware encryption must be to AES-256
- Unless there is a valid business reason why another standard must be used instead
- e.g. FileVault on Macs only encrypts hard drives to XTS-AES-128, but as the native integrated encryption application for Macs, this should be considered acceptable.

2.3 Cloud storage services

Confidential data stored on non-LSE-provided Cloud storage services must be encrypted at rest (e.g. by mounting a VeraCrypt volume on the service, or by encrypting individual files or archives).

2.4 Manual key management

Where keys are manually managed (e.g. passwords to encrypted files):

- The key must at least meet the minimum standards of LSE's Password Policy (e.g. at least 8 characters, including one lowercase, one uppercase and one numeral)
- The key is the responsibility of its generator
- The end user must understand that the loss of the key will result in the irretrievable loss of the data
- The key must be available upon legal request, in accordance with the Regulation of Investigatory Powers Act (2000)
- If the key must be transmitted, it will be transmitted using a different medium to the associated encrypted entity

2.5 Non-Centralised backups

All backups not using LSE's centralised backup service must be encrypted, or made to an encrypted volume or device.

2.6 Encryption and cross-border controls

Wherever possible, confidential information that requires encryption at rest will be held inside the organisation (e.g. at our onsite or Slough datacentres) and remotely connected to via a secured route such as LSE's SSL VPN. It is to be noted that some contractual agreements require us to specify in advance where data will be held.

Where this cannot be the case, either because VPN traffic is blocked (such as in Iran, China) or because the data must be collected *in situ* in areas without Internet access, and consequently it will be required to take confidential and encrypted data across borders, careful consideration must be made of the territories that will be visited and what measures must be taken both to protect data, and the safety of the researcher. Seek advice from information security and estates security if this is the case.

2.7 Non-compliance

- Failure to comply may lead to prosecution under UK law, breach of the General Data Protection Regulation or data supplier agreements.
- Failure to comply also breaches LSE's Conditions of Use of IT Facilities at LSE and may lead to disciplinary action.

2.8 Further resources

LSE provides further information on encryption considerations and techniques:

- How do I encrypt my stuff?
- Encryption guidelines
- Encryption guidelines for students
- Using 7zip to encrypt and decrypt files

2.9 Incident Handling

If a member of the School (staff or student) is aware of an information security incident then they must report it to the Information Management and Technology Service Desk at IT.Servicedesk@lse.ac.uk or telephone 020 7107 5000.
If necessary, members of the School can also use LSE's Whistle Blowing (Public Interest Disclosure) policy (see http://www2.lse.ac.uk/intranet/staff/brightIdeas/haveYourSay/whistleBlowing/Home.aspx.)

2.10 Review and Development

This policy, and any subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.
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

Responsibilities

IMT

- Providing encryption software as required
- Implementing hard drive encryption on laptops
- Encryption of network traffic between applications, systems and servers
- Corporate encryption key management
- Implementing encryption as appropriate in new corporate systems

IMT Information Security

- Encryption standards
- Encryption guides and advice
- This policy

End Users

- Encrypting files, folders or volumes when required, such as:
    - A requirement of a research data provider that data is encrypted at rest, or when it is transmitted, or both
    - Taking sensitive personal data out of LSE
    - Holding sensitive data on a mobile device such as a laptop or phone (where possible, encrypt the storage or hard drive)
    - You could be required to send personal data to another organisation
    - You want a higher degree of security around sensitive files held on site – exam questions, for instance

- Maintaining awareness of what constitutes personal data – contact the IMT Service Desk if you are unsure – and treating it accordingly (see the Information Classification Standard for more details)
- Handling the password management for File, Folder, and Volume encryption that you perform yourself
- Finding a method of sending password keys to others who require them that is not the same as the original method of transmitting the file – e.g., if you sent the file by email, you send the password by text

Document control

Version history

Date	Version	Comments
04/12/17 04/12/17	1.0 1.1	

Contacts

Position	Name	Email	Notes
Assistant Director of Cyber Security & Risk Management	Jethro Perkins	j.a.perkins@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	No
Will training needs arise from this policy	No
If Yes, please give details	