London School of Economics & Political Science

IT Services

Policy

Remote Access Policy

Jethro Perkins

Information Security Manager

Summary	This document outlines the controls from ISO27002 that relate to the LSE's Information Security Policy and Infrastructure that apply to the LSE, across all departments.
Version	Release 1.1
Date	dd month yyyy
Library reference	ISM-PY-105

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3	12/03/13	Jethro Perkins
Information Classification Standard	3	12/03/13	Jethro Perkins
Encryption Guidelines	1	22/01/13	Jethro Perkins

Version history

Date	Version	Comments
25/01/13	0.2	Initial version

Review control

Reviewer	Section	Comments	Actions agreed

Table of contents

1 Introduction

Mobile working provides benefits to LSE, its employees and students by enhancing communication; supporting flexible working practices; enabling new modes of study, scholarship and research; and facilitating the more efficient and effective use of time.

However the proliferation of mobile computing devices and remote access methods, and the increasing threats from malware and hackers, mean that information is increasingly at risk of being stolen, lost, leaked, inappropriately copied, or corrupted.

This combination of factors puts LSE, users of LSE systems and stakeholders dependent on LSE systems at risk of breaching ethical, legislative, regulatory and contractual requirements.

The Department of Information and Management Technology aims to provide the opportunities for secure, safe, accessible and available remote access and mobile working through its systems and policies, through the provision of technical controls on information access and through raising user awareness and encouraging good working practices.

This Policy aims to outline what resources IMT currently provides by default for remote use, and the responsibilities incumbent upon remote access users.

1.1 Purpose

The primary purposes of this policy are to:

1. Outline the resources LSE makes available by default for remote use.

2. Highlight that, although a resource may be available for remote use, the onus still remains on the end user to assess whether remote use is appropriate for any particular information.

3. Ensure that all users understand their own responsibilities for protecting the confidentiality, integrity and availability of the data that they handle remotely. This includes assessing how confidential their data are using the Information Classification Standard and then consulting the available guidelines or IMT's service desk for more help, if necessary.

4. Protect LSE from liability or damage through the misuse of its IT facilities.

1.2 Scope

This policy applies to all authorised users and the data/ information held, processed or controlled by or on behalf of LSE.

It covers the provision of the systems available for access remotely.

LSE does not make provision for all its IT systems and services to be made available remotely. Where the need for confidentiality or integrity of data is extremely high, such as when handling data classified as 'Confidential', remote access will be explicitly denied on request of the data owner, or as contractually demanded.

Users should be aware that the availability and speed of remote access is subject to a number of external factors beyond LSE's control, such as the effectiveness of any Internet Service Provider leased line, or any third party supplied router, firewall, or anti-virus software in being able to create and maintain a connection to LSE systems and services.

1.3 Definitions

Remote Access: accessing LSE systems from outside of LSE premises with an LSE owned, privately owned or publicly accessible computer, laptop, smart phone or other device. The information accessed and processed continues to reside on LSE systems or systems provided by third parties on behalf of LSE.

Mobile Working - carrying out work (i.e. the creation, storage, processing and transport or transfer of data/ information) as an employee of LSE from outside of LSE premises.

2 Responsibilities

Members of LSE:
All members of LSE, LSE associates, agency staff working for LSE, third parties and collaborators on LSE projects will be users of LSE information, and may use information remotely or using mobile devices. This carries with it the responsibility to abide by this policy, and its principles and any relevant legislation, supporting policies, procedures and guidance. It also carries the responsibility to assess the risk to information and handle it appropriately. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so.

Any access to LSE information is also governed by LSE's Conditions of Use.

Principal Investigators, Departmental Managers
Responsibility for ensuring that appropriate information can be accessed remotely and that, if necessary, additional safeguards to the access of data are requested.

School Secretary
Responsible for LSE compliance with the Data Protection Act

Department of Information Management and Technology, Library IT and STICERD IT Staff:
Responsible for ensuring that the provision of LSE's IT remote infrastructure is consistent with the demands of this policy, the Information Security Policy, and current good practise.

Information Security Manager:
Responsible for this and subsequent information security policies and will provide specialist advice throughout the School on information security issues.

Information Security Advisory Board
Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee
Responsible for approving information security policies.

3 Policy

3.1 List of default services remotely available to LSE users

This is current provision and may be amended at any time.

1. MS Exchange LSE email
2. Current Remote Desktop service. Provides remote access to:
   a. Microsoft Office (Access, Excel, Frontpage, Outlook, PowerPoint, Publisher, Word)
   b. Email,
   c. H: space
   d. password change tool
   e. Current standard desktop applications
3. LSE For You
4. VPN (map Outlook, H: space, any other shared drives). The current solution is due to be replaced by a dedicated VPN solution during 2013.
5. Moodle
6. Library system
7. Online recruitment system

3.2 System Administrator Access available remotely

Remote access to system administrator functions should be protected by two-factor authentication. This is not currently in place: a project will be created in order to address this.

3.3 Third party remote access

Remote access provided to third parties in order to e.g. remotely administer systems should be restricted to particular IP addresses, should involve a named account and the account should be disabled when it is not in use.

3.4 Information Assessment

The primary considerations for all members of the LSE community when either using remote access services, or working from a mobile device, are:

1. Know what data / information you are using
2. Consider what level of data classification should or does apply to it (for more information on how to classify the data that you hold, please refer to LSE's Information Classification Standard)
3. Understand and act upon any particular contractual, ethical or other requirement attached to the information
4. Consider how the mobile devices and the information you are processing can be managed in accordance with their information classification, or if they can't, how you can explicitly accept and manage the risk.

If, after you assess your information, you are not comfortable with the conditions your information is held in, or how it can be accessed remotely, please talk to IMT about any steps that can be taken to improve the situation.

3.5 Guidelines for remote and mobile working with 'Confidential' information

Please see the *Remote Access and Mobile Working Guidelines*

3.6 Device Theft and information Breaches

Please report the theft of any device holding ‘Confidential’ or ‘Restricted’ information, or any loss of or suspected inappropriate access to ‘Confidential’ or ‘Restricted’ information, to the IT Service Desk (IT.Servicedesk@lse.ac.uk).

3.7 Compliance, 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*.

3.8 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE’s overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE’s website via the Information Security Policies, Procedures and Guidelines page. 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.

3.9 Review and Development

This policy, and its subsidiaries, 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.