Policy

Access Control Policy

Jethro Perkins
Information Security Manager

Table of contents

1   Introduction

LSE implements physical and logical access controls across its networks, IT systems and services in order to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy.

Access control systems are in place to protect the interests of all authorised users of LSE IT systems by providing a safe, secure and accessible environment in which to work.

1.1   Scope

This policy covers all LSE networks, comms rooms, IT systems, data and authorised users.

1.2   Out of Scope

The LSE external website and other information classified as 'Public'.

Systems outside IMT control will not fall under Sections 3.2.1 and 3.2.2

2   Policy

2.1   Principles

LSE will provide all employees, students and contracted third parties with on-site access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

2.1.1   Generic identities

Generic or group IDs shall not normally be permitted as means of access to LSE data, but may be granted under exceptional circumstances if sufficient other controls on access are in place. Under all circumstances, users of accounts *must* be identifiable in order for LSE to meet the conditions of its Internet Service Provider, JISC (as laid out in the JISC 'Acceptable Use Policy').

Generic identities will *never* be used to access Confidential data or Personally Identifiable Data, including data supplied to LSE by HSCIC.

2.1.2   Privileged accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

Authorisation for the use of such accounts shall only be provided explicitly, upon written request from a senior manager (such as a head of department/division, or a departmental or centre manager), and will be documented by the system owner. Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity (such as may happen via Ransomware attacks, which typically are able to encrypt user data after silently installing on a machine over which the user has admin privileges, or the creation of further user accounts) .

2.1.3   Least privilege and need to know

Access rights will be accorded following the principles of least privilege *and* need to know.

2.1.4   Maintaining data security levels

Every user should understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to their sensitivity. The Information Classification Standard enables users to classify data appropriately and gives guidance on how to store it, irrespective of security mechanisms that may or may not be in place.

Users electing to place information on non-IMT-managed systems and databases, digital media, cloud storage, or removable storage devices are advised by IMT only do so where such an action is in accord with the information's security classification, or where other protective measures (such as the use of encryption) have been implemented. Users are consequently responsible in such situations for ensuring that appropriate access to the data are maintained in accord with the Information Security Policy and any other contractual obligations they may have to meet.

Users are obligated to report instances of non-compliance to the LSE via the IT Service Desk.

2.2   Access Control Authorisation

2.2.1   User accounts

Access to LSE IT resources and services will be given through the provision of a unique user account and complex password.

2.2.1.1 Staff User Accounts

Staff user accounts can only be requested in writing, and by using the appropriate forms, by departmental managers.

No access to any LSE staff IT resources and services will be provided without prior authentication and authorisation of a user's LSE account.

By default staff are provided with access to h: space (with access denied to all other users), and an email account.

They have access to a standard suite of software applications and the remote.lse.ac.uk portal.

By default staff accounts will expire upon termination of contract, unless a request for an extension is received from the relevant Departmental Manager.

2.2.1.2 Taught Postgraduate and Undergraduate Student User Accounts
By default taught postgraduate and undergraduate students are provided with access to h: space (with access denied to all other users), and an email account.

They have access to a standard suite of software applications and the remote.lse.ac.uk portal.

By default taught postgraduate and undergraduate students accounts will expire 2 months after the end of the course.

2.2.1.3 Research Postgraduate Student User Accounts
By default research postgraduate students are provided with access to h: space (with access denied to all other users), and an email account.

They have access to a standard suite of software applications and the remote.lse.ac.uk portal.

By default research postgraduate students accounts will expire at the end of the term following a successful viva.

2.2.1.4 External Collaborators

External collaborators will be provided access through the External Collaborator Access Framework. By default, this service provides *no access to LSE systems*. Only systems explicitly connected to the service by IMT will be able to use it. Collaborator accounts are issued and managed by LSE Sponsors, who will be system owners or, in the case of SharePoint, site owners.

Other collaborators requiring the creation of LSE Associate accounts (e.g. for the use of shared folders held on \\deptshared) will be governed by the LSE Associate Accounts Policy and accompanying processes.

2.2.1.5 Third parties

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles.

The accounts will be removed at the end of the contract or when no longer required.

Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

2.2.2   Passwords
Password issuing, strength requirements, changing and control will be managed through formal processes.

Password issuing will be managed by the IT Service Desk for staff and IT Helpdesk for students. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects. The criteria for both staff and student passwords are given at:
http://www2.lse.ac.uk/intranet/LSEServices/IMT/infosec/yourLsePassword.aspx

Password changing can be performed on LSE workstations, via LFY or the remote desktop.

2.2.3   Access to Confidential, Restricted and Internal Use information

Access to 'Confidential', 'Restricted' and 'Internal Use' information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreement or the *Information Security Policy*. The responsibility to implement access restrictions lies with the data and systems owners.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within LSE's Active Directory domains and administered by IMT.

There are no restrictions on the access to 'Public' information.

2.2.4   Policies and guidelines for use of accounts

Users are expected to become familiar with and abide by LSE policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the Conditions of Use of IT Services at LSE and the JISC acceptable use policy.

2.2.5   Access for remote users

Access for remote users shall be subject to authorization by IMT and be provided in accordance with the *Remote Access Policy* and the *Information Security Policy*. No uncontrolled external access shall be permitted to any network device or networked system.

2.3   Access Control Methods

Access to data is variously and appropriately controlled according to the data classification levels described in the *Information Security Policy*.

Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, user account privileges, server and workstation access rights, firewall permissions, network zone and VLAN ACLs, IIS/Apache intranet/extranet authentication rights, LSE login rights, database access rights, encryption and other methods as necessary.

Access control applies to all LSE-owned networks, servers, workstations, laptops, mobile devices and services run on behalf of LSE.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within LSE's Active Directory domains.

2.4   Cloud Systems

The use of cloud-based systems by LSE must in all respects meet the access control provisions laid out in this policy.

Evaluation of access controls implemented in any cloud system is performed during the vendor assessment and implementation stages of any project, via the completion by business analysts, project managers and cloud vendors of IMT's Cloud Assessment Questionnaire.

All completed cloud questionnaires are assessed by the Information Security Team, with appropriate remedial actions recommended or risks to be accepted before use is authorised.

2.5   Penetration Tests

LSE's access control provision will be regularly made subject to penetration tests, in order to ascertain the effectiveness of existing controls and expose any weaknesses. Tests will include, where appropriate and agreed to, the systems of cloud service providers.

2.6   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. 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.

A full list of existing information security policies can be found at:
http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/home.aspx.

2.7   Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IMT if required to ensure that it remains 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.

3   Responsibilities

Members of LSE:
All members of LSE, LSE associates, agency staff working for LSE, and alumni may have or require access to LSE data or IT systems, and may be responsible for the systems upon which LSE data reside.

System Owners
Those with responsibility for systems (including designating access) upon which LSE data reside. This includes but is not limited to Finance, HR, Registry, Library, STICERD.

Department of Information Management and Technology:
Responsible for:
- administering access to LSE's Active Directory environment and many of its systems
- hardening end user systems in accordance with research data provider requirements
- implementing role based access control upon the School's shared access file systems,
- creating LSE's Active Directory user accounts and passwords
- maintaining LSE's network infrastructure, firewalls and network zoning
- maintaining the External Collaborators Access Framework
- Project Management Office procedures for issuing and assessing Cloud Questionnaire responses, integrating the Cloud Questionnaire with project management tasks

Information Security Manager:
Responsible for writing this policy and establishing access control principles.

Information Security Team
Responsible for:
- assessing Cloud Questionnaire responses, with signoff on whether cloud systems can be used
- investigating breaches and recommending remedial actions
- organising annual penetration tests

Estates Security
Responsible for:
- Physical security on campus
- Administration of door access control systems
- Security of comms rooms and onsite datacentre

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.

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3.7	01/07/15	Jethro Perkins
Information Classification Standard	3.0	15/03/13	Jethro Perkins

Version history

Date	Version	Comments
27/03/13	0.1	Initial version
23/04/13	1.0	Released to ISAB
07/05/13	1.1	Incorporating changes requested by ISAB
18/06/13	1.2	Correction of inaccuracy in Section 3.2.1.1
10/07/15	1.3	Comprehensively updated to include issues around use of Cloud Service, the remote.lse.ac.uk service, use of Penetration Testing to assess control effectiveness, and the External Collaborators Access Framework. Responsibilities also updated.
30/10/15	1.4	Corrections and clarifications (particularly around generic accounts and responsibilities towards secondary data)
06/11/15	1.5	Formatting and spelling corrections. Update of section 2.1.2 to further clarify who can request administrative accounts.

Review control

Reviewer	Section	Comments	Actions agreed
ISAB	1.2	Some non-IMT systems do not fall within the remits of 3.2.1 and 3.2.2	Out of scope extended to reflect this comment
ISAB	3.2.1.2 and 3.2.1.3	By default students do not have access to shared departmental drives.	Document updated to reflect this
Mike Bragg	3.2.1.1	Departmental share permissions are not set as default. They are largely granted by the folder owners and their delegates.	Claim that permissions on departmental shared areas was provided by default has been removed.
ISAB	2.1.2	Further expansion and clarification required of who can request admin accounts.	Clarification provided in the body of the text.