THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Technical

Access Control Policy

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, as well as data provided by third parties, by creating a safe, secure and accessible environment in which to work.

Scope

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

Out of Scope

The LSE external website and other information classified as ‘Public’.
Privileged access to non-DTS controlled systems, resources and applications is the responsibility of the system, resource or application owner, *not* DTS. The authorisation and auditing processes involved in granting access to these resources is the responsibility of the resource owners.

Policy

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.

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 to identify the account user.

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 Information, including data supplied to LSE by NHS Digital.

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.

Privileged accounts must not be used for standard activities; they are for program installation and system reconfiguration, *not* for program use, unless it is otherwise impossible to operate the program.

Least privilege and need to know

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

Maintaining data security levels

Every user must understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user must still 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-DTS-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
- the provision meets any research data supplier or other contracts,
- 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 from data providers they may have to meet.

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

Access Control Authorisation

User accounts

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

Accounts are provided on the basis of valid records in the HR and student information systems. For any user not in either of those systems, access is granted via the appropriate staff or associate form signed by a Head of Department of Departmental manager. Default access is granted only to H: space, a personal OneDrive and an email account.

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 criteria for both staff and student passwords are given at: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/internal/staffAndStudents/pasPol.pdf

Password changing can be performed via https://myaccount.microsoft.com/.
Self Service password reset can be performed via https://passwordreset.microsoftonline.com/

MFA

MFA is switched on for all accounts.

Access to Confidential and Restricted information

Access to 'Confidential' and 'Restricted' information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreement with interested parties (e.g. NHS Digital and other research data providers) or the *Information Security Policy*.

Access to any of these resources will be restricted by use of firewalls, network segregation, secure log-on procedures, access control list restrictions and other controls as appropriate.

The responsibility to implement access restrictions lies with the data processors and data controllers, but must be implemented in line with this policy.

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 and Azure Active Directory domains and administered by DTS.

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

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.

Access for remote users

Access for remote users shall be subject to authorization by DTS 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.

Physical access control

Physical access across the LSE campus, where restricted, is controlled primarily via LSE Cards. Access to Comms Rooms is additionally restricted via the Comms Room Policy.

Lost cards

Lost LSE Cards must immediately be reported to the School's Security Office. The Security Office will cancel the card through the School's physical access control system.

Reissuing cards

Replacement cards cannot be issued until the Security Office has confirmed that a prior card has been cancelled. New cards with the same level of access control will be issued through the Library.

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 used by default include:

- explicit logon to devices,
- Windows share and file permissions to files and folders,
- user account privilege limitations,
- server and workstation access rights,
- firewall permissions,
- network zone and VLAN ACLs,
- IIS/Apache intranet/extranet authentication rights,
- LSE user login rights,
- Database access rights and ACLs,
- Encryption in flight
- Multifactor authentication
- Any other methods as contractually required by interested parties.

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 and Azure Active Directory domains.

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 of DTS's Cloud Assessment Questionnaire, filled in by business analysts, project managers and cloud vendors.

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. Where risks are deemed too large for the Information Security Team or the project in LSE commissioning the cloud service, the project will be referred to LSE's COO for approval.

Cloud systems must meet LSE's Minimum Standards for Cloud systems.

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.

Version history

Date	Version	Comments
21/10/14	1	Draft for comment
22/10/16	1.1	Updated after review
18/07/22	1.14	Revised and updated

Review schedule

Version:0.2 22/10/2020

DTS reference: ISM-PY-111

Review interval	Next review due by	Next review start
3 years	Jul 2025	June 2025

Contacts

Position	Name	Email	Notes
Director of Cyber Security and Risk	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**