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.

Governance

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
- Cancelling LSE cards

Library
Issuing new library cards

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.

Governance

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.
20/01/16	1.6	Inclusion upon advice from the Audit Committee and HR of section 2.2.6 on LSE cards. Updated responsibilities accordingly.
08/02/16	1.7	Corrected 'Out of Scope' reference to correctly point at 2.2.1 and 2.2.2 (as opposed to 3.2.1 and 3.2.2). Also updated Out of Scope to explicitly address systems, applications and other resources outside IMT control, as requested by Rachael Hope of HR on the suggestion of the Audit Committee.

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.

Rachael Hope	1.2	Explicit reference needed to be made to the way users of non-IMT resources are granted elevated privileges over the resources.	Wording updated to better reflect the responsibilities involved.