2 Policy

2.1 Principles

The LSE will operate a physically secure network, protected as far as is practical from tampering or snooping by malicious parties.

2.1.1 General Communications Room environment

Standards relating to the general design and construction of Communications Rooms shall be found in the Estates Specification for Capital Developments. Communications Rooms will have solid doors, which close automatically. These doors will not have signs which indicate their purpose, but just the official room code.

2.1.2 Least privilege

Access rights will be accorded following the principles of least privilege. Access to Communications Rooms will be limited to only those persons with a legitimate purpose for such access.

2.1.3 Dedicated use

Communications Rooms are dedicated solely for the provision of data networking services, and must not be used for other purposes (e.g. storage or thoroughfare to other areas).

2.2 Physical security

Physical security of Communications Rooms will be managed in accordance with LSE Security standards and policies and with the Access Control Policy.

Communications Room doors will be secured with a Salto lock. Requests for authorised access via Salto keys will be handled by LSE Security. LSE Security will only process requests for access from either authorised LSE staff, or where the IMT Networks Team has approved the request.

Audit records of access to individual Communications Rooms via Salto key will be retained by Security for 3 months.

2.3 Authorised access

The following LSE staff will be permitted access to Communications Rooms at any time:

- IMT Networks Team
- Estates Facilities
- Estates Security

Requests for other parties (e.g. contractors) to access Communications Rooms can be made to the IMT Networks Team, with one weeks' advance notice.

Where urgent access to a Communications Room is required by a non-authorised person, they may be permitted access if escorted at all times by an authorised member of staff.

2.4 PCI DSS standards

The processing of credit card data on the LSE network requires that the LSE complies with relevant PCI DSS standards, described in the LSE's PCI DSS Compliance Policy

The physical security of all Communications Rooms will meet relevant PCI DSS requirements, in order to permit credit card data to be processed wherever there is a legitimate business need.

2.5 Incident Handling

If a member of the School (staff or student) is aware of unauthorised access to a Communications Room, or of unauthorised equipment within a Communications Room, 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.)

2.6 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

IMT Networks
Authorisation of access to Communications Rooms.
Management of data cabling and active network equipment within Communications Rooms.

Estates Division
Consulting with IMT Network Team when designing Communications Rooms.
Managing Salto key access to Communications Rooms for authorised staff.
Maintaining audit logs of Salto key access to Communications Rooms.

Document control

Distribution list

Name
Information Security Advisory Board Information Technology Committee

External document references

Title	Version	Date	Author
Estates Specification for Capital Developments		2016	Martyn Fisher
Access Control Policy	1.7	08/02/2016	Jethro Perkins
PCI DSS Compliancy Policy	1.3	17/11/2014	Jethro Perkins
Information Security Policy	3.11	09/12/15	Jethro Perkins

Version history

Date	Version	Comments
23/05/2016	1	Approved by Information Technology Committee 05/12/16

Review control

Reviewer	Section	Comments	Actions agreed