1 Introduction

Most core activities at LSE rely heavily upon its IT network, including: teaching, research, administration, HR and Finance functions, building management, access control and CCTV. It is, as a consequence, essential that the stability, integrity and security of the network are safeguarded for use by all members of LSE's community.

1.1 Purpose

This policy will assist in ensuring the availability of an effective, highly available network. It provides formal responsibilities for taking measures against devices that threaten the stability, integrity and security of LSE's network. It will facilitate the rapid tracking down and resolution of problems related to LSE network connected devices by Information Management and Technology.

1.2 Scope

All devices connected to LSE's IT network

2 Responsibilities

Director of Information Management and Technology
Responsibility for authorising the investigation or disconnection of any system or device threatening the stability, integrity or security of the network.

IMT Information Security Manager
Operational responsibility as delegated by the Director of IMT for requesting the investigation or disconnection of any system or device threatening the stability, integrity or security of the network.

IMT Information Security Team
Organising penetration tests and vulnerability scanning. Receiving, assessing and acting upon (where appropriate) reports from Janet CSIRT,other incident response teams or law enforcement agencies.

IMT Networks
Disabling and re-enabling devices or equipment network access as appropriate. Blocking and unblocking inbound and outbound network traffic as appropriate. Throttling available network bandwidth to systems, services, applications, devices and network segments. Investigating as required any system or device as directed by the Information Security Manager, or as governed by any applicable procedures or other policies. Explicit approval of distribution layer connections performed by other individuals, teams or organisations.

IMT Systems and IMT Support Teams
Investigating as required any system or device as directed by the Information Security Manager or as governed by any applicable procedures or other policies.

System and device owners
Maintaining system integrity, updating Operating Systems and applications with security and other critical patches, ensuring appropriate access to systems using 'least privilege' and 'need to know' principles, reporting any issues to IMT.

All LSE network users
All users of the network must be aware that they are bound by the LSE Information Security Policy, the Conditions of Use of IT Facilities at LSE and the JANET Acceptable Use Policy.

3 Policy

3.1 Network addresses

All network addresses, including IP addresses and DNS Names, will be allocated and administered by IMT. Any allocated IP addresses and DNS Names may be removed under the instruction of the Information Security Manager.

3.2 Physical connections to LSE network

Physical connections to the LSE network edge switches or backbone may be made only by IMT or otherwise with the explicit permission of the IMT Network team. No extensions or modifications to the physical infrastructure of the LSE network, including wireless, may otherwise be made. This includes the addition of:

- network switches
- hubs
- wireless access points
- router devices
- cabling other than connecting a patch cable to a provided network wall socket.

3.3 Control of LSE network infrastructure and bandwidth

All network infrastructure equipment or network wiring at LSE will be managed and controlled by IMT.

IMT may, on behalf of the School, restrict excessive use of network bandwidth by any system or service.

3.4 Third Party Equipment

Third parties may be permitted to connect devices to the Network to provide services to LSE and its users following due consultation with IMT in order to assess the consequences for the School's Network and its security.

3.5 Systems threatening the stability, integrity and security of the network

In the event where LSE IMT has discovered or otherwise been informed that a system on the LSE network is threatening the stability, integrity or security of the network, or has otherwise been compromised, hacked, is sending out malicious traffic or is the source of SPAM or other issues that affect the stability, integrity or security of the LSE network, IMT has the right to:

- gain access to and inspect the configuration of devices or equipment
- take remedial actions as necessary
- remove from the network any devices or equipment that it believes could be the source of the problem, or otherwise block inbound and outbound traffic, as appropriate.
- disable as necessary any part of the network in order to remove the source of the problem

Whilst every effort will be made to contact the system owner, Head of Department and/or other appropriate persons, this may not always be possible. All services will be reconnected at the first opportunity after the problem has been remediated.

3.6 Failure to comply

In all cases, a failure to comply that threatens the stability, integrity or security of the network or has caused a breach of such will be dealt with by:

1. Stopping the damage
2. Stopping the risk
3. Remediating the cause

3.7 Penetration tests

To proactively protect the security and operation of the network and the systems thereon, IMT may carry out both manual and automated systematic vulnerability scans and penetration tests on computer systems connected to the School network. Best efforts will be undertaken to minimize any disruption, and any unavoidable or unrecoverable damage will be investigated.

3.8 Incident Handling

If a member of the School (staff or student) is aware of an information security incident 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.)

3.9 Review and Development

This policy, and any subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain 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