LSHTM Information Management and Security Policy

Supporting Policy 4: Network Connection and Management Policy

Endorsed by Academic Affairs - Feb 2014

1. Introduction

This policy forms part of the LSHTM Information Management and Security Policy and, as such, is binding on all members of the School.

2. Scope

This policy will cover all equipment, irrespective of ownership, attached to the School data network whether directly through wired connections, or using wireless technologies or by making virtual connections using a virtual private network (VPN) and their use within the Acceptable Use Policy.

3. Responsibilities for all network users

3.1 New connections of equipment to the School network may only be made with the authority of IT Services. Users are permitted to plug in client machines, but must not extend the network in any way.

3.2 Users must not advertise wireless networks within the LSHTM estate. This means users must not connect anything that will act as a wireless access point.

3.3 Access to the School network must not be shared with unauthorised users.

3.4 Connected equipment must be maintained in accordance with manufacturers' recommendations. Operating system and application software must be kept up-to-date to ensure risk from security vulnerabilities is minimised. Equipment must not be, or remain, connected to the network after a manufacturer ceases to provide security patches without the prior approval of the Head of IT Security, IT Audit and Compliance.

4. Management of the network

4.1 The School's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. Where network infrastructure is not managed by IT

Services, read-only access to devices must be provided to IT Services, on request, for the purpose of ITS being able to monitor the entire network. All network management staff shall be given relevant training in information security issues.

4.2 IT staff creating services must register all IP addresses in use with an appropriate entry in the Domain Name System and this registration must be kept up-to-date.

4.3 Appropriate logs must be kept so that it is always possible to determine who/what was using a particular IP address at a particular time. Logs should be retained for 3 - 6 months in compliance with LINX Best Current Practice - Traceability[1].

4.4 Machines must be disconnected from the network when requested by ITS. Such requests are typically when a system has caused problems to other users of the network or to an external network and/or following a security breach. Systems must ***not*** be reconnected to the network without the explicit authorisation of the IT Security team.

4.5 The protocols currently approved by the School for use over their network are those comprising the Internet Protocol suite. Any other protocols (e.g. AppleTalk) must be approved by ITS.

4.6 In the event of unacceptable network events occurring on a LAN, or in order to safeguard the security of other systems, ITS has the right to gain access to and inspect the configuration of devices or equipment on that network and to require the immediate removal of any devices or equipment that it believes could be the source of the problem. ITS also has the right to disable any or all of the LAN, as necessary, to diagnose and/or remove the source of the problem.

5. Design

The network must be designed and configured to deliver high performance and reliability to meet the organisation's needs whilst providing a high degree of access control and a range of privilege restrictions.

6. Security

6.1 The network must be segregated into separate logical domains with routing and, where appropriate, access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting the organisation's business systems.

6.2 All parts of the School will be protected by an institutional firewall.

6.3 At a minimum, a policy of 'default deny inbound' and 'default permit outbound' will apply at an institutional firewall. Servers which are required to be accessible from outside the School will need to be registered and approved by IT Security. IT Services will require full details of the server and data to be stored on it, as well as details of the system owner. IT Services reserve the right to run security tests on the server and require that any vulnerabilities are addressed **prior** to any access being granted.

---

[1] LINX Best Current Practice at https://www.linx.net/good/bcp/traceability-bcp-v1_0.html

6.4 New applications and systems must transmit and/or accept passwords or other authentication credentials only if strongly encrypted. Existing uses of clear-text authentication should be disabled as rapidly as practicable. If this is not possible, IT Security must be contacted for advice.

6.5 IT Security have the right to disconnect systems considered insecure.

7. Network access

7.1 Access to the resources on the network must be strictly controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

7.2 Remote access to the network will be subject to robust authentication and VPN connections to the network are only permitted for authorised users ensuring that use is authenticated and data is encrypted during transit across the network.

7.3 Moves, adds, changes and other reconfigurations of users' network infrastructure will only be carried out by IT Services according to procedures agreed within IT Services.

8. Wireless

8.1 All wireless access to the School network must be authenticated and logged. As for wired infrastructure (s 4.3), appropriate logs must be kept so that it is always possible to determine who/what was using a particular IP address at a particular time. Logs should be retained for 3 - 6 months in compliance with LINX Best Current Practice (as in 4.3 above).

8.2 Requirements for new wireless connectivity should be arranged with IT Services.

8.3 Users must not advertise wireless networks within the LSHTM estate. This means users must not plug in anything that will act as a wireless access point even if they do not connect to the School network, as they may still interfere with other wireless provision and/ or provide unsecured access to the Internet and, thus, risk to the School. IT Security retain the right to disable (without notice) any 802.11[2] wireless device they identify as being unauthorised.

9. Status of this document

This document is a part of LSHTM's information security policy and has been approved by Senior Leadership Team/Academic Affairs Committee. It is subject to regular review.

---

[2] Set of standards relating to wireless networks