Information Security Policy

London School of Hygiene & Tropical Medicine

Contents

1. Version Control

Version Number	Author	Purpose/Change	Date
1.0	Jim Nicholas (Information Security Manager)	Temporary Policy Review	5/2/20

2. Summary

2.1 Objectives

2.1.1 The purpose of this information security policy is to empower LSHTM to pursue its primary objectives unhindered by the threats the university faces. This policy and its sub-policies are created to mitigate these risks efficiently and effectively.

2.1.2 This policy identifies what LSHTM values (its assets) and defines what security properties (e.g. confidentiality, integrity & availability) they must maintain. It governs asset management. Assets, including but limited to, infrastructure, hardware, software, records (digital and paper) and people must be appropriately managed throughout their LSHTM lifecycle.

2.1.3 It ensures all relevant users are aware of and comply with the policies, legislation and agreements appropriate for their role and responsibilities.

2.1.4 This document defines the process of developing policy which is approved by the senior management at LSHTM. They are committed to the protecting the university's assets and adherence to its obligations. The development and regular review of this policy is the foundation of this process.

2.2 Scope

2.2.1 The policy applies to all users and entities that process data under direction from LSHTM. This policy must be read, understood and complied with by all relevant users including but not limited to students, staff, contractors and visitors.

2.2.2 This policy is the top-level document of LSHTM's Information Security Management System (ISMS). Its aim is to be concise and non-technical to enable all relevant users to understand and comply with it. The ISMS provides a set of sub-policies, standards and procedures to appropriately manage LSHTM data. Relevant documents will be sign-posted throughout this policy.

3. Policy

3.1 Development

3.1.1 This policy has been approved by the Information Governance Board (IGB). This decision-making body is responsible for defining and reviewing information governance objectives. Once the policy is approved by the Management Board, it will become LSHTM policy and binding on all departments.

3.1.2 The IGB may make available supplementary procedures and codes of practice and promote them throughout LSHTM. Once approved by the Management Board, these will also become LSHTM policy and will be binding on all departments. The IGB will also arrange for analysis of security assessments received from departments and report on these to Management Board.

3.2 Review

3.2.1 This policy (and its sub-policies) are reviewed once per year. If there is a major change in LSHTM systems and it is deemed to impact the directives of this policy, a review may be conducted within a shorter timeframe.

4. Legal & Regulatory Obligations

4.1 Legislation

4.1.1 The university, each member of staff, and its students have an obligation to abide by all UK and relevant EU legislation. Of importance in this respect are:

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA)
- Human Rights Act 1998
- Investigatory Powers Act 2016
- The Investigatory Powers Regulations 2018.

4.2 Responsibilities

4.2.1 The requirement for compliance devolves to all users, who may be held personally responsible for any breach of legislation. Relevant legislation is referenced in supporting policies. For full details see here: http://www.legislation.gov.uk.

4.3 Data Protection

4.3.1 LSHTM has defined responsibilities for managing sensitive data in accordance with the DPA and GDPR. These responsibilities are documented in the Data Protection Policy.

4.3.2 All students, staff and others who may process sensitive data under LSHTM direction must read and comply with the Data Protection Policy. For queries regarding this policy contact the Data Protection Officer (dpo@lshtm.ac.uk).

4.3.3 If a data breach is suspected you must report the potential breach immediately. For further details see the Data Protection Policy.

5. Classification

5.1 What is classification?

5.1.1 Classification is the process of analysing and labelling data (digital or paper) according to the impact a compromise of its confidentiality, integrity and/or availability would have on LSHTM. The greater the impact, the higher the classification. 4 Levels of classification are used by LSHTM: Public, Internal, Confidential & Highly Confidential.

5.1.2 For definitions of these classifications and when to apply them refer to the Data Classification & Handling Policy. All staff, students and relevant others must read and comply with this policy.

5.2 Why must data be classified?

5.2.1 Without appropriate classification and labelling, data will likely be inconsistently managed. This inconsistency may lead to sensitive data being processed in inappropriate ways, potentially leading to a damaging data breach.

5.2.2 Classification enables efficient processing of data. The significant amount of data most organisations process is not very sensitive. If data is not classified, to comply with legal requirements it would be necessary to handle all data as if it was very sensitive. This adds restrictive protections, creating unnecessary demands to many common tasks.

5.3 Who must classify data?

5.3.1 Data owners are responsible for classification. Heads of departments are commonly considered data owners. However, data owners are more broadly defined as those that create the data. Data owners must classify and appropriately label data according to LSHTM's Data Classification & Handling Policy. For further guidance on data ownership contact the DPO (dpo@lshtm.ac.uk).

6. Hardware & Software Management

6.1 Lifecycle

6.1.1 All hardware and software used to process data under the direction of LSHTM must be registered in IT Services Asset Management System. This is to ensure appropriate management of its lifecycle.

6.1.2 IT Services publishes a catalogue of recommended devices. If practicable, it is required to select one of these proposed products. This is to promote standardisation which in turn enables efficient, appropriate management of the asset. All non-standard devices require approval by IT Services.

6.1.3 All hardware and software not directly supplied by ITS which may be used for the processing of sensitive data must be approved by ITS. This is to provide oversight on the appropriateness of the proposed solution.

6.1.4 Throughout the use of the hardware or software asset, it must be supported with adequate security patches by the vendor. These patches must be applied within 2 weeks in the case of Critical or High-Risk vulnerabilities.

6.1.5 An essential part of the asset lifecycle is managing its end of life. An end of life must be recorded on the Asset Management System before rollout. Once the asset has reached this stage is must be appropriately disposed of. Any sensitive data must be secure destroyed. For advice contact the Information Security Manager (csirt@lshtm.ac.uk).

6.1.6 Due to lifecycle demands it is necessary for appropriate budgeting to be included in project planning and funding applications.

6.1.7 When users leave LSHTM IT assets must be returned to LSHTM for re-use or destruction.

6.2 Services

6.2.1 If a new service is proposed it is required that a request is submitted to the Service Design Authority (SDA). This process is to review requirements to review if they can be met with current LSHTM systems. If they cannot be adequately met, then guidance on an appropriate solution will be provided. To submit a request, contact the Service Desk.

6.3 Records Management

6.3.1 The LSHTM Records Management Policy applies to all records created, received or maintained by staff of the School in the course of carrying out their corporate functions. Records and documentation created in the course of research, whether internally or externally funded, are also subject to contractual and/or other legal record-keeping requirements. The LSHTM Archivist and Records Manager is responsible for the secure storage of non- current and archive files. Contact the Archive & Records Manager for guidance.

7. Acceptable Use

7.1 Acceptable Use Policy

7.1.1 All staff, students and others authorised to access LSHTM's systems and data must read, understand and agree to the Acceptable Use Policy (AUP). This policy governs use of all devices connected to LSHTM's network and accessing 3rd party services on behalf of the university.

7.1.2 All users must register with IT Services to provide accountability in the case of policy violations. All access is granted via a user account for our staff, students & authorised visitors. In addition, restricted Wi-Fi can be accessed by those with eduroam accounts from other institutions.

7.1.3 The AUP must be agreed by all users before access to LSHTM's systems and services can be granted. It is the responsibility for all line and managers and relevant tutors ensure this is adhered to.

7.2 Email

7.2.1 All staff and students should only use LSHTM email systems approved by IT Services for sending and receiving email on behalf of LSHTM. This is necessary to ensure the university can control the data it is responsible for.

7.2.2 Reasonable, moderate and lawful personal use of LSHTM email systems is permitted. However, the university may revoke this privilege if the use is deemed inappropriate or otherwise not in line with LSHTM policy.

7.2.3 You may not use LSHTM provided systems to send spam, chain letters or material which is offensive, inappropriate, defamatory, threatening, illegal or may otherwise violate any of the university's policies.

7.2.4 All current instances of email servers hosted within or on behalf of LSHTM must be registered with and approved by IT Services.

7.2.5 All users and administrators of LSHTM email services must read and comply with the Use of Email Policy.

7.3 Network

7.3.1 Any machine using the LSHTM network (wireless or wired, local or remote) is subject to and must comply with the Network Connection & Management Policy. All users connecting a device to LSHTM's network that has not been provisioned, configured and managed by IT Services must read and comply with the Network Connection & Management Policy.

7.3.2 It is forbidden to connect any networking device such as but not limited to switches, routers, hubs and access point without formal, documented consent from the Head of Networks. Any non-compliant devices at any time of our choosing and without consultation may be removed by IT Services.

7.4 Bring Your Own Device

7.4.1 Using personal devices in the workplace is becoming increasingly common. LSHTM staff and students often work with sensitive data. Tasking unmanaged personal devices with working on sensitive data creates significant for the university and its objectives. To manage this risk while maintaining reasonable flexibility it is required all users work must read and comply with the Bring Your Own Device Policy.

8. Monitoring

8.1 Maintenance & Security

8.1.1 To maintain the confidentiality, integrity and availability of IT services at LSHTM it is necessary to monitor the network and connected systems. When connecting devices to the LSHTM network or logging on to the university's services users must be aware and accept there may be logs recorded of that connection. Only necessary and proportionate monitoring is conducted for the maintenance and security of LSHTM assets.

8.2 Additional Responsibilities

8.2.1 In addition to monitoring for maintenance and security purposes IT Services may be requested to monitor individual activities. This will be proportionate, follow

due process and appropriately authorised.

8.2.2 Unauthorised monitoring must not be conducted and may result in prosecution. For further information and legal obligations regarding monitoring refer to the Monitoring & Security Policy.

9. Information Security Awareness

9.1 Introductory Information

9.1.1 Staff with supervisory responsibility shall ensure their staff and/or students have undertaken the mandatory Information Security Awareness training. In addition to the required data protection training.

9.2 Additional Training & Support

9.2.1 For additional training requirements contact the Information Security. Presentations, 1-2-1 and group workshops and technical skill shares can be delivered but due to time constraints it is recommended to discuss this at the earliest possible time.

10. Advice & Reporting Data Breaches

10.1 IT Support

10.1.1 For general IT help please use the ServiceDesk portal https://servicedesk.lshtm.ac.uk or contact our IT Helpdesk on ext. 5000.

10.2 Information Security

10.2.1 For information security alerts and requests email csirt@lshtm.ac.uk. To contact the Information Security Manager directly call Ext. 8396

10.3 Reporting Data Breaches

10.3.1 Any loss or suspected breach involving personal data (digital or paper) must be reported immediately to the Data Protection Officer (dpo@lshtm.ac.uk) and the Information Security Manager (csirt@lshtm.ac.uk).

10.3.2 All physical security breaches (e.g. thefts, losses, break-ins, on or off site) should be reported to Information Security Manager (csirt@lshtm.ac.uk).

10.3.3 If there is a potential breach of research data, in addition to notifying the DPO

and Information Security Manager it will be necessary to notify RGIO (rgio@lshtm.ac.uk)