

JOB DESCRIPTION



Job Title: Information Security Manager
Department: Information Technology Services
Faculty/Central Service: Central Services
Location: Keppel Street, London
Reports to: Director of IT Services
Responsible for: 1 x Senior Information Security Officer (Grade 6) 1 x Information Security Officer (Grade 5)
Full Time/Part Time/Casual: Full time
Grade: Grade 7
Overall Purpose of the job: To be responsible for the determination, planning, design, development, organisation, implementation and evaluation of information security processes, systems and policies across the School. This includes tracking business requirements, and collaborating with colleagues involved in the School audit, and colleagues involved with risk and compliance
To be responsible for the overall operational effectiveness of our cybersecurity monitoring, detection, and response capabilities. This role acts as the primary liaison between our organisation and the outsourced MDR/SOC partner. You will ensure the partner meets defined service level agreements (SLAs), drive continuous improvement in detection capabilities, manage incident escalation paths, and ensure the security strategy aligns with business goals
To be responsible for ensuring that an information security framework is in place and carrying out will carry out risk assessments and internal audits of all IT products and services both in IT services and also across the LSHTM to ensure the efficacy of our Information Security posture
They will also actively promote Information Security compliance through training, campaigns and engagement. They will take the lead in co-ordinating and responding to formal information access requests and complaints within the sphere of IT products and services.
The role will also be pivotal in enabling the delivery and continuous improvement of all information security management activities related to the University, both operational and strategic projects, services and systems with an IT component.
The role will direct project (including research projects) stakeholders on how to be compliant with the required due diligence activities, and will ensure information security work packages are completed to a both a General Data Protection Regulation (GDPR) compliant standard, and as required by the Group's Information Governance Group.

General Information

The London School of Hygiene & Tropical Medicine (LSHTM) is one of the world's leading public health universities.

Our mission is to improve health and health equity in the UK and worldwide; working in partnership to achieve excellence in public and global health research, education and translation of knowledge into policy and practice.

Staff and students are committed to helping create a more healthy, sustainable and equitable world for everyone, because we believe our shared future depends on our shared health.

We embrace and value the diversity of our staff and student population and seek to promote equity, diversity and inclusion as essential elements in contribution to improving health worldwide. We believe that when people feel respected and included, they can be more creative, successful, and happier at work. While we have more work to do, we are committed to building an inclusive workplace, a community that everyone feels a part of, which is safe, respectful, supportive and enables all to reach their full potential.

To find out more please visit our [Introducing LSHTM page](#).

Our Values

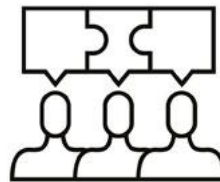
Our values establish how we aspire to achieve our mission both now and in the future - demonstrating what it means to work and study at LSHTM. Please visit our [LSHTM Values page](#) for further information.



**Act with
integrity**



**Embrace
difference**



**Work
together**



**Create
impact**

Main Duties and Responsibilities

The post holder will have an excellent understanding of relevant standards (e.g. ISO 27001-2013), legislation (e.g. GDPR), licensing models and compliance and audit best practice. They will apply this insight to enable the business to operate safely and efficiently.

The post will be line-managed by the Director of IT Services and will work closely with all areas of the institution in order to ensure Information Security compliance across LSHTM and the Africa Units.

Information Security runs to the heart of every aspect of the operation of the LSHTM and it is essential that the operation of all IT services are delivered in a manner that protects LSHTM, and in particular protects all personal and confidential data and information, which must also comply with all relevant regulations and legislation.

The IT department itself is a significant business operation and the post holder is expected to have a good understanding of the business operation of LSHTM and the services ITS delivers to it and the relationships in place with the customers and suppliers of the department. In addition the post holder should have a good understanding of administration and financial management within a large and complex IT environment supporting a University.

The role holder will be part of the IT Services Senior Management Team (ITS-SMT). Out-of-hours work is an occasional requirement of the role for either planned or unplanned operations.

This role involves:

- Sets out and defines a strategic management model for IT and digital information compliance based on business objectives, adopted standards or regulatory requirements.
- Drafts and maintains the policy, standards and procedures for compliance with relevant legislation.
- Creates and maintains an inventory of information assets, which are subject to relevant legislation. Prepares, reviews and submits periodic notification of registration details to the relevant regulatory authorities. Ensures that formal information access requests and complaints are dealt with according to approved procedures.
- Setting strategic direction for Information Security.
- Provides authoritative advice and guidance on the application and operation of controls, including legislative or regulatory requirements relating to the above.
- Takes responsibility for compliance with any relevant statutory, internal, or external regulations, standards, and codes of good practice relating to
 - information and records management
 - information security
 - data protection
 - licensing of software
 - procurement
 - contract and supplier management
- Development and maintenance of information security policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice (PCI-DSS, GDPR, DPA, FOI etc).

- Management and assessment of threats to confidentiality, integrity, availability, accountability and relevant compliance. Takes ownership of security control reviews, business risk assessments, and reviews that follow significant breaches of security controls.
- Operation of appropriate security controls as a production service to business system users.
- Provide expert advice and guidance relating to security matters in the development and maintenance of the IT services business continuity planning and LSHTM IT disaster recovery planning
- Management of IT security audits both internal and with the assistance of external security specialists. Ensuring any remedial actions are carried out in an effective and timely manner.
- Implementation of best practice to ensure security, whilst maintaining business needs, through the application of formal protection measures
- Management of information security risk assessments; the development of realistic measures to mitigate any identified risks.

In addition, there are the following ITS-SMT Shared Responsibilities:

- Provide strategic direction for a team of technical staff within the IT Services Division.
- Provide a primary point of contact for IT Services.
- Communications; act as the central reference point for all internal and external communications for the teams within their group.
- Ensure all department staff are compliant with School policies and procedures and provide direction to staff in relation to these.
- Responsibility for fully managing the yearly capital and project budgets assigned to their group within IT Services.
- Liaison; on an ongoing and as-required basis act as a representative for IT Services within the wider School community. This may include for instance attending faculty and departmental meetings, acting as a communications conduit between academic and administrative staff and IT Services.
- Creation of business cases for new service requirements as part of the LSHTM planning round.
- Acting as a full-time member of the IT Services Senior Management Team (ITS-SMT).

- Liaising with senior level stakeholders at LSHTM to ascertain Cyber Security needs and support requirement.
- Ensuring all relevant Management Information for the services they manage are made available for ITS-SMT, and feed into wider discussions relating to improvement requirements.

Additional Information

- Adhere to faculty and school policy and procedures at all times.
- Demonstrate continuous personal and professional development by acquiring and refining relevant skills and expertise in new or related areas, through internal or external development activity.
- Contribute to general activities of the department and school that help to promote the objectives of the school.

Generic duties and responsibilities of all LSHTM employees

This job description reflects the present requirements of the post but may be altered at any time in the future as duties and responsibilities change and/or develop providing there is consultation with the post-holder.

The post-holder will carry out any other duties, tasks or responsibilities as reasonably requested by the line manager, Dean of Faculty, Head of Department or Head of Professional Service.

The post holder will be responsible and accountable for ensuring all LSHTM policies, procedures, regulations and employment legislative requirements are adhered to including equality and diversity and health and safety.

This job description is not a definitive or exhaustive list of responsibilities but identifies the key responsibilities and tasks of the post holder. The specific objectives of the post holder will be subject to review as part of the individual Performance and Development Review (PDR).

PERSON SPECIFICATION

This form lists the essential and desirable requirements needed by the post holder to be able to perform the job effectively.

Applicants will be shortlisted solely on the extent to which they meet these requirements.

Competency	Evidence	E / D
Education, Qualifications and Training	<ul style="list-style-type: none"> • Hold relevant professional qualifications or equivalent experience • Hold an undergraduate degree or equivalent 	<p>E</p> <p>D</p>
Experience	<ul style="list-style-type: none"> • Proven ability to provide inspirational leadership and direction to a group of highly technical IT professionals, demonstrating a high degree of personal credibility • Substantial relevant managerial experience of delivering Information Security and Compliance Services. • Strong line management skills, including motivating, performance management, influencing and negotiating. • Substantial relevant experience in a Higher Education institution or similar environment. • Strategic planner –business and technical. • Proven experience of exerting influence at a senior level, alongside the ability to provide strategic vision and direction to colleagues and peers • Ability to deliver to strict targets and deadline, showing a comprehensive understanding of financial management • Proven change management skills in complex environments. • Proven advanced analytical and problem-solving skills • Experience of effective budgetary management and control, and ability to understand and produce financial costings and reports. • Experience of contributing to operational and strategic planning. 	<p>E</p> <p>E</p> <p>E</p> <p>E</p> <p>E</p> <p>E</p> <p>E</p> <p>E</p> <p>E</p> <p>E</p>

	<ul style="list-style-type: none"> • Experience of preparing and facilitating internal and external IT audits. • Proven experience in providing support to a range of stakeholders. • Experience of introducing and monitoring compliance with policies, procedures, processes and systems. • Excellent written and oral communication skills including proven ability to present financial and other information in a clear and logical format and draft documentation. • Using a network of key individuals to secure important business information and influence broad organisational change 	<p>E</p> <p>E</p> <p>E</p> <p>E</p> <p>E</p>
Knowledge	<ul style="list-style-type: none"> • Specific skills & knowledge of information security, data protection, compliance, financial management, related legislation and regulations • Highly developed knowledge of the principles, theory and practices of IT management as well as an awareness of broader methodological developments relevant to information technologies • Well-developed knowledge of IT systems and services and how they relate to each other • Well-developed understanding of regulations and legislation relating to information technologies and information management and governance and the implications of non-compliance to regulations/legislation 	<p>E</p> <p>E</p> <p>E</p> <p>E</p>
General	<ul style="list-style-type: none"> • A focus on results – consistent delivery of projects on time and to specification • A collaborative and flexible approach with evidence of ability to work independently with minimal supervision and as part of a team. • Well-developed communication skills: verbal, written and via presentations. The ability to sell ideas or benefits and build persuasive arguments based on data, logic and the objective merits of solutions • Excellent interpersonal skills, including the ability to establish effective working relationships with staff and students from a wide variety of backgrounds; the ability 	<p>E</p> <p>E</p> <p>E</p> <p>E</p>

	<p>to communicate technical issues to non-technical users effectively</p> <ul style="list-style-type: none"> • A high degree of personal motivation, including the ability to work independently and organise priorities • Proven ability to pro-actively use initiative, judgement and creativity to solve problems and to propose and implement ways of working more efficiently or effectively. • The ability to look continuously for opportunities for improvement and to develop strategies for change to influence and shape the future direction of the business – adapting thinking and behaviour to suit the requirements of different situations • Commercial awareness and the ability to lead vendor contract activities effectively • Display a professional attitude towards colleagues, students and others at all times and in all communications 	<p>E</p> <p>E</p> <p>E</p> <p>D</p> <p>D</p>
--	---	--

E-Essential: Requirement without which the job could not be done

D-Desirable: Requirements that would enable the candidate to perform the job well

Date compiled: April 2026

Salary and Conditions of Appointment

The post is permanent and full-time 35 hours per week, 1 FTE. The salary will be on the LSHTM salary scale, Grade 7 scale in the range £53,317 - £61,034 per annum pro rata (inclusive of London Weighting).

The post will be subject to the LSHTM terms and conditions of service. Annual leave entitlement is 30 working days per year, pro rata for part time staff. In addition to this there are discretionary "Wellbeing Days." Membership of the Pension Scheme is available.

LSHTM operates a Hybrid Working Framework which, alongside agreed service requirements, enables teams to work more flexibly where the role allows - promoting wellbeing and a better work/life balance. Please note that roles based in London are required to work on-site a minimum of two days per week.

Application Process

Applications should be made on-line via our [jobs website](#). Applications should also include the names and email contacts of 2 referees who can be contacted immediately if appointed. Online applications will be accepted by the automated system until 10pm of the closing date. We regret that late applications cannot be accepted. Any queries regarding the application process may be addressed to jobs@lshtm.ac.uk.

The supporting statement section should set out how your qualifications, experience and training meet each of the selection criteria. Please provide one or more paragraphs addressing each criterion. The supporting statement is an essential part of the selection process and thus a failure to provide this information will mean that the application will not be considered. An answer to any of the criteria such as "Please see attached CV", "Yes" or "No" will not be considered acceptable and will not be scored.

Please note that if you are shortlisted and are unable to attend on the interview date it may not be possible to offer you an alternative date.

Asylum and Immigration Statement

LSHTM will comply with current UKVI legislation, which requires all employees to provide documentary evidence of their legal right to work in this country prior to commencing employment. Candidates will be required to email a copy of their passport (and visa if applicable) to HR prior to their interview and if appointed will be asked to bring the original documents in to be copied and verified before their start date.

Applications from candidates who require sponsorship to work in the UK will be considered alongside other applications. Applicants who do not currently have the right to work in the UK will have to satisfy UK Visas & Immigration regulations before they can be appointed.

Further information about Sponsorship and eligibility to work in the UK, can be found on the [government immigration rules page](#).