THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Job Description

This form summarises the purpose of the job and lists its key tasks. It is not a definitive list of all the tasks to be undertaken as those can be varied from time to time at the discretion of the School, in consultation with the postholder.

Job title: Information Security Analyst

Department/Division:	**DTS**
Accountable to:	**Information Security Manager**

Job Summary:

The main purposes of the Information Security Analyst role are to be responsible and accountable for performing second line of defence incident response, vulnerability management, threat detection and response, PCI DSS audit and other audit tasks, establishing the implementation of appropriate system, network and data controls; commissioning annual penetration test and internal vulnerability scan, attacks and data breaches; participating in projects as required and providing consultancy on best practice; operational control of information security tools.

The Information Security Officer will be working very closely with the Information Security Manager and will be expected to take the lead in assessing data management plans, user safety, security control implementation, handling threats and issues, monitoring compliance, and advising end users over information security issues. It is essential that, along with a strong knowledge of information security concepts and approaches, the post holder is able to engage with a wide range of staff with differing backgrounds and technical competencies and has a knowledge of the higher education environment.

Reporting to the Information Security Manager they are responsible for:

Responding to information security threats, vulnerabilities, attacks and requests

- To deal with reports of cyber security incident, compromised systems and user accounts, whether these reports originate from external bodies (such as JISC or other CSIRT teams) or internally
- Monitor alerts from LSE’s existing SIEM tool and optimise the tool where necessary
- Liaise with the third party managed SIEM service and carry out investigations as necessary
- Monitor alerts from the threat detection and response tool (end point security and M365 security) and carry out investigation as necessary
- To coordinate where necessary with other teams, departments and external bodies to close vulnerabilities, eliminate threats and investigate breaches
- To update, amend and create School-wide incident response processes as required
- To respond as required to other requests for information either from within the School or from external bodies, as directed by the Information Security Manager
- To actively monitor against information security threats and take appropriate action to mitigate them

Penetration Testing and vulnerability assessments

- Commission the independent annual penetration tests and vulnerability assessments, lead and follow up on the remediation actions
- Carry out a monthly internal system scans and report back to the relevant business areas, provide recommendations as appropriate

- Manage regular vulnerability scanning and reports to appropriate business areas.

Consultancy on Best Practice

- Working with researchers and professional staff in order to provide them with advice on best practice in information security, based on data supplier requirements, relevant legislation, ISO27001 standards, Cyber Essentials, NHS Data Security and Protection Toolkit requirements and PCI DSS as appropriate
- Dealing with information assurance requests from research data providers
- Other advice as appropriate around personal safety and security, both off and on campus

Security Posture Assessment

- Conduct annual PCI DSS audits
- To audit and / or investigate as required the cyber security posture of services and systems within LSE, or run by LSE in cloud environments
- To assess services and systems against known standards e.g. Cyber Essentials, NHS DSPT
- To advise on the protection of systems administered outside DTS

Skill Requirements

- Proven experience of information security incident response
- User experience of SIEM tools
- Evidence of carrying out information security investigations
- Good understanding of the OWASP Top Ten and mapping OWASP vulnerabilities onto real-world applications
- A level of understanding of Information Security Standards including ISO27001, PCI DSS, Cyber Essentials
- Understanding of relevant legislation affecting the delivery of IT services (e.g. GDPR, Computer Misuse Act, RIPA)
- Strong analytical skills
- Ability to organise and prioritise work in an effective manner
- Ability to work under pressure and unsupervised
- A methodical and disciplined approach to work
- Good general knowledge of IT infrastructure environment(s)

Duties/Responsibilities

Communication

- Excellent report writing, presentation and verbal skills are mandatory
- Use a range of communication skills and methods to raise and maintain awareness of information security to all members of the School
- Respond both in person and in writing to requests for advice on information security from any member of the LSE community
- Write guidelines for the School-wide use of information security technologies
- Ensure members of DTS as appropriate understand their involvement in information security procedures and processes

Teamwork and Motivation

- Work with other DTS colleagues and colleagues from other departments to resolve incidents
- Work with business areas across the School to conduct PCI DSS audits and other spot checks as required

- Work with technical teams and business areas across the School to remediate on findings from the annual penetration test and internal vulnerability scans
- Work with other members of the School to provide advice and help as required

Liaison and Networking

- Work with outside consultants as directed by the Information Security Manager to carry out independent security audits and penetration tests
- Work with groups inside the School in order to raise and address information security issues
- As directed by the Information Security Manager, work with the Estates Security Team and, if appropriate, members of the security services in order to complete investigations into incidents that arise on campus or that involve members of the LSE community
- Work to make sure principles of information security are embedded across the School
- Ensure colleagues know where to go to obtain information about security policies, process, procedures and guidelines

Knowledge and Experience

- Understanding of information security concepts and principles
- Knowledge of information security standards and relevant legislation affecting the delivery of IT services
- Good understanding of information security vulnerabilities and threats
- Experiences of operational security with a good level of technical skills
- Understanding of core IT operations and experience of SIEM tools
- Experience of problem solving using own initiative
- Experience liaising with a wide range of stakeholders

Service Delivery

- Respond quickly and effectively to new threats and vulnerabilities.
- Analyse vulnerabilities and implement remediations
- Deliver audits against predefined standards or frameworks
- Working with the appropriate technical operational managers, ensure adequate vulnerability, threat, patch information tracking and analysis
- In the event of a security breach or other incident, ensure that any necessary evidence is secured and as directed by the Information Security Manager undertake appropriate measures to prevent further damage
- Conduct potentially confidential investigations School-wide as instructed by the Information Security Manager. This could involve access to extremely sensitive and/or distressing material

Decision Making Processes and Outcomes

- Review all information security incidents and issues, solve where possible, escalate or liaise where necessary with the appropriate internal or external bodies
- Prioritise and manage workload effectively, with minimal supervision

Planning and Organising Resources

- Plan spot checks and other audit activities as directed by the Information Security Manager
- Recommend to the Information Security Manager, DTS teams and business-led IT any appropriate changes to existing provision

Initiative & Problem Solving

- Determine the most appropriate course of action to solve problems within existing constraints
- Draw together disparate leads in order to understand an issue
- Recommend changes and innovations to existing provision where appropriate
- Attention to detail

- Ability to perform investigations including through interviews and by collating appropriate evidence
- Strong time management and self-motivational skills
- Use own initiative and work independently in order to solve issues

Analysis & Research

- Ability to analyse and research new security issues, vulnerabilities and incidents within the LSE context.
- Knowledge of appropriate legislation and when it should be applied
- Keep abreast of new developments within information security
- Identify and raise risks with the Information Security Manager and other members of the LSE Community as appropriate

Flexibility

To deliver services effectively, a degree of flexibility may be required in the duties performed in order to meet the exigencies of service. Job roles may also naturally develop over time and ongoing substantial changes to a role will be discussed between line managers and their staff, with job descriptions updated as and when appropriate.

Equity, Diversity and Inclusion (EDI)

LSE is committed to building a diverse, equitable and truly inclusive university. All posts (and post holders) will seek to ensure diversity and inclusion, while opposing all forms of unlawful and unfair discrimination on the grounds of age, disability, gender identity, marriage and civil partnership, pregnancy and maternity, race, nationality, ethnic or national origin, religion or belief, sex and sexual orientation, or social and economic background.

Ethics Code

Posts (and post holders) are assumed to have a responsibility to act in accordance with the School's Ethics Code and to promote the principles and values that the Code enshrines. The Ethics Code clearly states that the whole LSE community, including all staff, students, and governors of LSE, are expected to act in accordance with the principles which are set out in the Code. As such you are required to read and familiarise yourself with it. The School's Effective Behaviours Framework is designed to support this Code. It sets out examples for the six behaviours that all staff are expected to demonstrate, these can be found on the following link: click here

Environmental Sustainability

The post holder is required to minimise environmental impact in the performance of the role, and actively contribute to the delivery of the LSE Environmental Policy.