

LONDON BOROUGH OF LEWISHAM

JOB DESCRIPTION

Designation:	IT Security Manager	Grade:	PO8
Reports to (Designation):	Head of IT Architecture & Security	Grade:	SMG3
Directorate:	Corporate Resources	Section:	IT & Digital Services

Main Purpose of the job:

Accountable as strategic lead for cyber and information security, you will identify and assure the security of the council's technology services, applications and digital solutions. You will lead in the evaluation of new projects, software and hardware products, and vendors, including examining vendor contracts and terms of service. You will support teams across the council to develop their understanding of security risk and data privacy issues.

You will take lead on Lewisham IT & Digital Services, as well as work with Shared Technology Services (STS) and other technology suppliers to put in place control over security systems, such as firewalls, data protection controls, patching, encryption, vulnerability scanning and penetration testing. You will be responsible for achieving compliance with Public Sector Network (PSN), Common Assessment Framework, and related government frameworks including those of the National Cyber Security Centre, the Information Commissioners Office (ICO) and Information Security for London.

Summary of Responsibilities and Personal Duties:

- Responsible for the monitoring all IT operations and infrastructure, including reviewing alerts and logs, ensuring the councils' technology remains secure.
- Accountable for creating an IT Security Strategy to embed good practice, and put forward a roadmap for improvements.
- Responsible for identifying and establishing the correct security tools to monitor application security.
- Accountable for monitoring internal and external policy compliance, ensuring that both vendors and employees understand the council's cyber security risk management policies and that they operate within that framework.
- Responsible for achieving compliance with Public Sector Network (PSN) and related government frameworks including those of the National Cyber Security Centre, the Information Commissioners Office (ICO) and Information Security for London.
- Responsible for working with MHCLG and other organisations to achieve the Council's CAF accreditation.
- Accountable for the security of new technology implemented across the council. Evaluate the suitability of the product, challenge vendors and internal teams to ensure security and risk is understood, accepted, and documented.
- You will continuously audit Lewisham's policies and controls, identifying options to improve or remediate.
- Accountable for creating and managing the technology security incident response program, ensuring applications across the council have Emergency Planning, Business Continuity and Disaster Recovery processes in place.
- Partner with the *Head of Information Security* and *Data & Analytics Manager* to support improving the quality, security and integrity of information gathering, recording and storage.
- Work with Shared Technology Services (STS) and other technology suppliers to ensure any cross-cutting projects or security impacts are considered.
- Stay up-to-date with new cyber security developments and services
- Design, build and maintain a framework for managing information assets, improving how information is captured, shared, accessed, stored, retained and disposed of.
- Detect and fight attacks and intrusions, minimising the potential damage incurred by security breaches.

- Report on security incidents, producing lessons learnt and actions for future mitigation, ensuring these actions are embedded for future improvement.
- Design and implement a robust IT test strategy across the council, ensuring that testing becomes embedded in the product lifecycle and adopts a risk based approach.
- Undertake a risk management function across the council, responsible for carrying out risk assessments across functional and technical areas within the council.
- Co-ordinate the development of countermeasures and contingency plans and manage the implementation of all agreed audit recommendations.
- Manage the business continuity function by managing risks to mitigate risks to the IT function.
- Ensure that the council can provide minimum agreed service levels in the case of disaster by reducing the risk to an acceptable level and planning for the recovery of IT services.
- Strategically advise Executive Directors and Heads of Service to ensure IT systems security and integrity.
- Strategically advise and report to members of the council and other senior officers or members.
- Undertake any other duties commensurate with the general level of responsibility of this post
- Take responsibility for own personal and professional development ensuring that technical knowledge and skills are current and meet the demands of the post.
- Comply with our legal responsibilities under the General Data Protection Regulation (GDPR), Freedom of Information Act, Environmental Information Regulations and the Privacy and Electronic Regulations and Information Security Standards.
- Carry out duties with due regard to the Council's Customer Care, Equal Opportunities, Information Governance, Data Protection and Health and Safety policies and procedures

Internal contacts:

These include Members, Executive Directors, Directors, Service Group Managers and other staff across the Council as appropriate

External contacts:

This will include 3rd party suppliers currently working with Lewisham, other IT suppliers, Government departments, other Public Sector organisations

To carry out the duties of the post with due regard to the Council's relevant codes and procedures.

All employees are required to participate in Appraisal and Performance Management processes and to undertake appropriate training and development, including mandatory induction training, identified to enhance their work.

Undertake other duties, commensurate with the grade, as may reasonably be required.

Consideration will be given to restructuring the duties of this post for a disabled postholder

THIS JOB DESCRIPTION MAY NEED TO BE AMENDED BY THE DIRECTORATE TO MEET
THE CHANGING NEEDS OF THE SERVICE.

Number of fully managed staff: 1

Title: Support Application Analyst - Security

Grade: PO5

No of posts: 1

Number of partially managed staff: 0

Title:

Grade

No of posts

PERSON SPECIFICATION

JOB TITLE: IT Security Manager

POST NO:

DIRECTORATE: Corporate Resources

GRADE: PO8

Note to Candidates

The Person Specification is a picture of the skills, knowledge and experience needed to carry out the job. It has been used to draw up the advert and will also be used in the shortlisting and interview process for this post.

Those categories marked 'S' will be used especially for the purpose of shortlisting.

Please ensure that Equality and Diversity issues are addressed specifically in relation to the role for which you are applying when addressing the requirements of this person specification where appropriate.

If you are a disabled person, but are unable to meet some of the job requirements specifically because of your disability, please address this in your application. If you meet all the other criteria you will be shortlisted and we will explore jointly with you if there are ways in which the job can be changed to enable you to meet the requirements.

NOTICE FOR THE MANAGER

You do not have to use all of the categories; they are included to provide guidance to you. However, it should be noted that under normal circumstances. It is usually only knowledge, experience and an awareness of Equal Opportunities issues which can be measured from the Application Form.

CATEGORY	ESSENTIAL REQUIREMENTS 'S'
<u>Equal Opportunities</u> To demonstrate commitment to the principles of equality and diversity in employment and service delivery.	S
<u>Knowledge and Experience</u> Extensive knowledge of all relevant legislation relating to the IT security and Information Governance area and how these must be applied to a local government setting Extensive knowledge of all IT security aspects, including; audit response, oversight and scrutiny, ICO responses, Information Governance, Information Assurance, IT Asset Management policies, Quality Assurance, Test Strategies, PSN and PCI and other relevant compliance frameworks including CAF, disaster recovery and business continuity. Experience of working in a complex IT support service within a large organisation.	S S S

Must have an in depth knowledge of local authorities or similarly complex organisations to understand the business impact of all decisions	S
Track record of achievement at a management level in a similarly large and complex organisation:	S
Experience of working within an IT security and Information Governance service.	S
Experience of developing, implementing and maintaining Security Governance Frameworks and Security Strategies, Policies and Standards	
Track record of successfully undertaking IT audits and responding to and implementing audit recommendations and findings.	
Experience of providing timely and appropriate responses to the ICO.	
Experience of dealing with and managing the impact of security breaches.	
Experience of operating within a Service Management environment and aligning IT security within this.	
Proven skills and a track record of delivering IT security solutions, including appropriate controls to large complex organisations.	
Demonstrable experience of influencing and delivering measurable outcomes in a large complex organisation	
Proven experience of proactively working on own initiative, under pressure to tight and potentially conflicting deadlines, managing and prioritising own workload	
<u>Qualifications</u> Educated to degree level or equivalent, with evidence of continuous professional or managerial development Evidence of on-going professional development. Knowledge of the IT Infrastructure Library (ITIL) framework	

<u>Personal Qualities</u> Skilled in managing and motivating people to achieve successful outcomes and deliver desired results Successfully able to lead and motivate people not under direct line management to deliver on IT security and governance requirements Ability to adopt an innovative approach to complex situations to react positively to problems and develop radical solutions to ensure all service requirements are met. Able to quickly understand underlying issues in complex situations and make recommendations and successfully implement solutions Proven ability to effectively communicate in writing and verbally, in simple non-technical language, complex concepts or situations to stakeholders at all levels across the Shared Service Skilled at removing technical jargon from explanations and explaining IT security and Information Governance issues in easy to understand language. Understanding businesses real and stated needs and ability to influence stakeholders, at all levels and manage expectations. Able to run meetings effectively, understanding and influencing the roles played by participants and responding to challenges positively Contribute to the longer term development of the service area and the wider Shared IT Service.	
<u>Circumstances</u> Able to attend meetings in the evening and, on occasions, work outside and beyond the normal office hours to ensure deadlines and business objectives are achieved	
<u>Physical</u> If you are a disabled person, but are unable to meet some of the job requirements specifically because of your disability, please address this in your application. If you meet all the other criteria you will be shortlisted and we will explore jointly with you if there are ways in which the job can be changed to enable you to meet requirements.	

DBS Disclosure Required?
No ☒
Basic ☐
Enhanced ☐

(Tick as appropriate – guidance available from your HR Advisor)