Job Profile comprising Job Description and Person Specification

Job Description

Job Title: Information and Cyber Security Analyst (Senior)	**Grade**: PO4 – PO6
Section: IT	**Directorate:** Chief Executive
Responsible to following manager: Information and Cyber Security Manager	**Responsible for following staff:**
Post Number/s:	**Last Review Date** 08/09/2023

Working for the Richmond/ Wandsworth Shared Staffing Arrangement

This role is employed under the Shared Staffing Arrangement between Richmond and Wandsworth Councils. The overall purpose of the Shared Staffing Arrangement is to provide the highest quality of service at the lowest attainable cost.

Staff are expected to deliver high quality and responsive services wherever they are based, as well as having the ability to adapt to sometimes differing processes and expectations.

The Shared Staffing Arrangement aims to be at the forefront of innovation in local government and the organisation will invest in the development of its staff and ensure the opportunities for progression that only a large organisation can provide.

Job Purpose:

As an Information and Cyber Security Analyst with focus on 1) infrastructure, email, data, and web security, or 2) applications and data security, your primary responsibility will be to safeguard the councils' digital assets and data against potential security threats and vulnerabilities. You will play a crucial role in ensuring the confidentiality, integrity, and availability of sensitive information within the applications, as well as protecting them from unauthorised access, data breaches, and cyber-attacks. This position requires a strong technical background, hands-on experience in secure infrastructure, email, web or applications development/deployment, and a deep understanding of security best practices.

Key Duties and Responsibilities:
The Duties and Responsibilities listed below are for the two main areas 1) and/or 2) mentioned above.

- Security Assessment and Vulnerability Management:
  - Contribute to ensuring security aspects in proposed third party IT systems/ applications or security solutions.
  - Conduct comprehensive security assessments and penetration tests on IT assets or changes to identify vulnerabilities and potential weaknesses.
  - Utilise various security testing tools and methodologies to perform application security assessment.
  - Monitor security vulnerabilities and threats related to applications and track remediation efforts.
- Secure SDLC Integration:
  - Encourage security by design into the software development lifecycle (SDLC) by collaborating with development/implementation teams to adopt secure practices.
- Identity and Access Management
  - Contribute to development and maintenance of RBAC policies and procedures to govern access rights within IT systems, applications, databases, and related systems.
  - Review or contribute to establishing secure Access Rights
- Threat Modelling:
  - Conduct threat modelling exercises to identify potential security risks and provide recommendations for risk mitigation.
- Security Policy Development:
  - Assist in the development and enforcement of security policies, procedures, and standards across the councils.
- Security Awareness and Training:
  - Develop and deliver security training to developers and other relevant stakeholders to promote a security-conscious culture within the organization.
- Security Monitoring:
  - Ensure security logging and monitoring are available as appropriate.
  - Participate in the incident response process to identify and mitigate security incidents affecting applications.
- Security Standards and Compliance:
  - Ensure compliance with relevant industry standards, regulations, and internal security policies.
  -
  - Adhere to security controls and requirements as mandated by the SSA's policies, procedures, and local risk assessments to maintain confidentiality, integrity, availability and legal compliance of information and systems.
- Security Solutions:
  - Design and contribute to configurations of new and existing security solutions.

- Research and Innovation:
    - Stay up to date with the latest security threats, vulnerabilities, and industry best practices.
    - Continuously enhance knowledge and skills through research and self-learning.
- Perform any other duties as required by management to ensure continued operation and security of the SSA IT.

Generic Duties and Responsibilities

- To contribute to the continuous improvement of the services of the Boroughs of Wandsworth and Richmond.

- To comply with relevant Codes of Practice, including the Code of Conduct and policies concerning data protection and health and safety.

- To adhere to security controls and requirements as mandated by the SSA's policies, procedures, and local risk assessments to maintain confidentiality, integrity, availability and legal compliance of information and systems.

- To promote equality, diversity, and inclusion, maintaining an awareness of the equality and diversity protocol/policy and working to create and maintain a safe, supportive and welcoming environment where all people are treated with dignity and their identity and culture are valued and respected.

- To understand both Councils' duties and responsibilities for safeguarding children, young people, and adults as they apply to the role within the council.

- The profile is not intended to be an exhaustive list of duties the post holder will carry out. Other reasonable duties commensurate with the level of the post, including supporting emergency and priority situations, will form part of the role.

Progression Criteria.

PO4: - Post holder would be expected to perform the duties of the post competently under a low level of technical supervision and to have the ability to spot situations where problems need to be referred up the management line for resolution. Experience of deputising for line manager where required. Some experience of being a technical lead in projects is required.

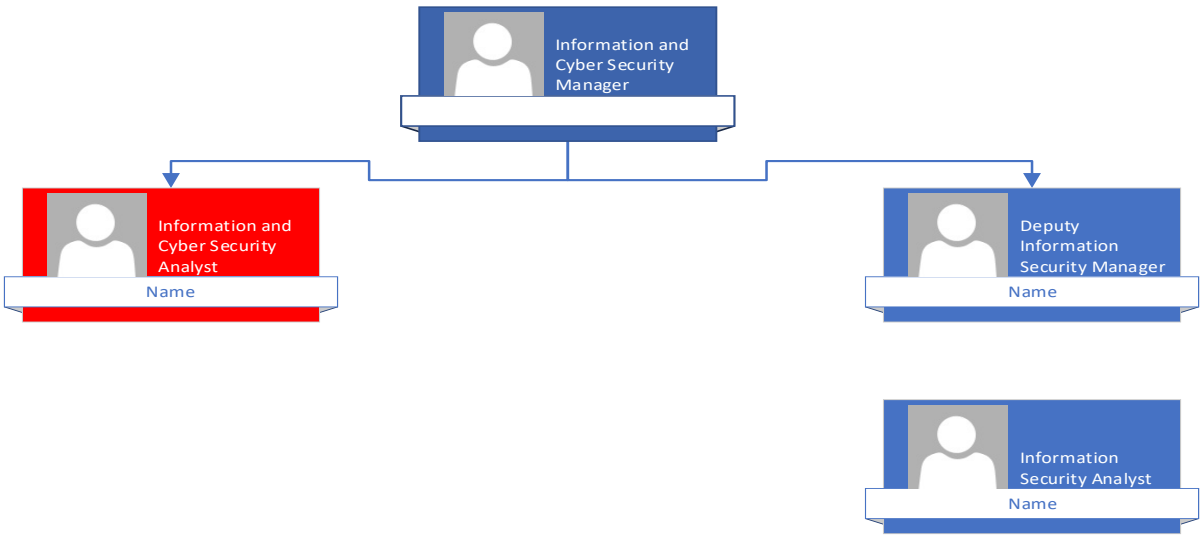
Conversant with the SSAs IT technologies and able to diagnose non-routine problems that involve more complex designs.

PO5 - A sufficient level of experience allowing duties of the post to be performed without direct technical supervision. The post holder should be able to proactively suggest ways of resolving non-routine issues. Some experience of leading immediate team both from a technical and operational perspective.

Conversant with the SSAs IT technologies and able to diagnose non-routine problems that involve more complex designs.

PO6 - A level of experience which enables the post holder to take charge of incidents and problems and see them through to resolution by troubleshooting, carrying out research and engaging further assistance where necessary without supervision. The post holder should have developed the personal and professional qualities necessary to provide a high level of input to the overall management of the IT service and to make recommendations to senior managers and to the Head of IT in relation to broader IT management issues where necessary. Post holder is expected to have managerial experience and, if necessary be able to deputise for the relevant team leader or senior manager.

Team Structure



Person Specification

LONDON BOROUGH OF RICHMOND UPON THAMES

Wandsworth number one for service and value

Job Title: Information and Cyber Security Analyst (Senior)	**Grade**: PO4 -PO6
Section: IT	**Directorate:** Resources
Responsible to following manager: Information and Cyber Security Team Manager	**Responsible for following staff:**
Post Number/s:	**Last Review Date**

Our Values and Behaviours

The values and behaviours we seek from our staff draw on the high standards of the two boroughs, and we prize these qualities in particular:

- **Being open.** This means we share our views openly, honestly and in a thoughtful way. We encourage new ideas and ways of doing things. We appreciate and listen to feedback from each other.
- **Being supportive.** This means we drive the success of the organisation by making sure that our colleagues are successful. We encourage others and take account of the challenges they face. We help each other to do our jobs.
- **Being positive.** Being positive and helpful means we keep our goals in mind and look for ways to achieve them. We listen constructively and help others see opportunities and the way forward. We have a 'can do' attitude and are continuously looking for ways to help each other improve.

Person Specification Requirements	**Essential**	**Desirable**	**Assessed by A / I/ T/ C** (see below for explanation
Knowledge			
Security Threats	**X**		**A/I**
Strong knowledge of common vulnerabilities, software security architecture, and common application security vulnerabilities (e.g., OWASP Top 10)	**X**		**A/I**
Knowledge of secure authentication and authorisation mechanisms (e.g., OAuth, SAML).		**X**	**A/I**
Experience			

Proven experience (typically 3+ years) in application security, software development, or a related security field (for Apps focus role)	**X**		**A/I**
Experience of vulnerabilities mitigation	**X**		**A/I**
Strong exposure to DLP		**X**	**A/I**
Strong Experience in Cloud Security (e.g. Azure) and Access Rights		**X**	**A/I**
Extensive experience working with SIEM products		**X**	**A/I**
Familiarity with industry standards and regulations (e.g., GDPR, NIST, PCI-DSS, NCSC for cybersecurity).	**X**		**A/I**
Skills			
Security Assessments/Reviews and Penetration Testing	**X**		**A/I**
Data Sensitivity Classification	**X**		**A/I**
Risk Analysis and Mitigation		**X**	**A/I**
Defender for Endpoint/Identity		**X**	
Demonstrated ability to look through large data sets to identify anomalies	**X**		**A/I**
Excellent communication and teamwork skills to collaborate effectively with cross-functional teams	**X**		**A/I**
Qualifications			
B.Sc. or M.Sc. degree or equivalent professional qualification in Computer Science, Information Security, or related field.	**X**		**A/C**
Certifications such as CISSP, CISM, CSSLP, CEH, CASE, or relevant incident handling and application security certifications are a plus.		**X**	**A/C**

A – Application form / CV
I – Interview
T – Test
C - Certificate