THE ROYAL BOROUGH OF KENSINGTON AND CHELSEA

JOB DESCRIPTION

Job title	**Security Architect**
Directorate	Chief Executive
Service	ICT
Team	Architecture and Governance
Grade	Grade I

DBS Check Required	Standard
Justification for DBS	Choose an item.
Politically Restricted	No

Responsible to:	Head of Service
Employees directly supervised *(if applicable)*:	None

Organisational structure chart *(job titles only, no employee names)*

1. JOB PURPOSE:

1. To act as the Council's senior technical authority on cyber security architecture and on the implementation of effective technical controls to mitigate the risks of cyber threats.
2. To design assure and oversee the implementation of secure and resilient solutions across a complex environment that includes legacy systems and modern cloud services.
3. To ensure the effective use of Microsoft security controls, including Azure Active Directory (AD), Defender, Intune, Conditional Access, Purview, and related technologies so that people only see the data that they need to in relation to their role.
4. To strengthen the council's security posture and support its transition to a zero-trust security model.
5. To review solution designs and advise on whether they meet council security standards, and if not, what to do to enable compliance, or on acceptable workarounds within the Council's risk tolerance.
6. To determine go / no go decisions in relation to technical security.

2. DESCRIPTION OF DUTIES:

Strategic security design

- Define and maintain up to date security principles for the Council, ensuring effective governance of the overall security of the Council's ICT estate.
- As a member of the Strategic Architecture Board and Technical Design Authority, work closely with the Lead Architect, Head of Cyber Assurance infrastructure teams, application teams, and suppliers to ensure that all technology decisions are secure, compliant, and aligned to the council's Digital, Data and Technology Strategy and Architecture principles.
- Provide professional security architecture design guidance for new systems, upgrades, changes, integrations, and migrations to ensure that the organisation's information assets remain secure and protected against cyber threats.
- Lead the security design of patterns, standards, and reference architectures.
- Ensure architectural decisions support the council's move toward Zero Trust, modern identity, and cloud-first principles.
- Act as the Council's subject-matter expert for Microsoft security technologies, including Azure AD / Entra ID, Microsoft Defender suite (Endpoint, Identity, Cloud Apps, Office 365), Intune / Endpoint Manager, Conditional Access, Microsoft Purview (DLP, Information Protection, Insider Risk), Sentinel and Log Analytics.
- Design secure configurations, policies, and controls that maximise the value of the council's Microsoft investment.
- Provide assurance and oversight for Microsoft-based security implementations and changes.
- Assure that built solutions meet the intended design.

Modernisation and risk management

- Assess and mitigate risks associated with legacy applications, unsupported systems, and technical debt.
- Develop secure-by-design approaches that work within the constraints of older technologies.
- Support the implementation of the ICT Strategy roadmap, ensuring successful secure migration paths to SaaS platforms.
- Sit on the Cyber Resilience Programme Board and provide strategic technical advice to it in relation to cyber controls.

Compliance

- Ensure solutions comply with relevant standards and frameworks, including:
  - National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)
  - Public Sector Network (PSN) Code of Connection
  - Payment Card Industry Data Security Standard (PCI DSS),where applicable
  - Data-protection and information-governance requirements

- Provide security assurance for major programmes, procurement, and supplier engagements.
- Lead threat-modelling, risk assessments, and security design reviews.

Stakeholder engagement

- Work with the Head of Cyber Resilience Lead Architect, and technical teams to design and embed security controls into all stages of ICT and project delivery.
- Provide clear, actionable advice to project managers, product teams, and service leads.
- Build strong relationships with suppliers and managed-service providers to ensure secure delivery.

Continuous improvement

- Monitor emerging threats, vulnerabilities, and best practice, advising on their relevance to the council.
- Promote a culture of secure design, secure configuration, and continuous improvement.
- Contribute to the development of security training, awareness, and human-risk initiatives by providing expert advice and input in relation to the latest technical threat landscape and mitigating controls, including delivering sessions and determining risks and training needs.
- Be committed to continuous professional development.

The duties and responsibilities outlined in this job profile are indicative of the role, however they are not exhaustive and may be subject to change. In addition, you will be required to undertake other reasonable duties as directed by your manager.

SELECTION CRITERIA/PERSON SPECIFICATION

Conditions to Note:
The person specification outlines the essential requirements the post holder or applicant must meet to fulfil the role and the duties outlined.

Candidates:
When completing your application form, please address your answers directly to each of the selection criteria below. This enables the panel to assess your ability to meet each criterion. It is essential that you give at least one example of your ability to meet each of the four Values and Behaviours: Putting Communities First, Respect, Integrity and Working Together.

Recruiting Managers:
The following values and behaviours are essential criteria in each post and must be addressed directly by candidates. The Guidance Notes on values and behaviours for managers give example questions to probe candidates in the interview and application stages of the recruitment process.

Resilience:
We encourage staff to assist the council during a significant emergency response which will focus on meeting the needs of residents. This may necessitate staff involvement, and in exceptional circumstances, could involve redeployment to support the emergency response.

Informed by our learning from the Grenfell tragedy, senior managers (Head of Service and higher) are expected to play an active coordination and leadership role in the Council's broader emergency response efforts during major or serious incidents. This includes arranging urgent resources from their own services and rallying staff teams to help residents during their time in need.

Values & Behaviours
The Royal Borough of Kensington and Chelsea have identified four key behaviours and values that should be demonstrated by all council employees. Successful candidates will show the ability to meet these behaviours.

A	**Equal Opportunities** Demonstrate an understanding of and commitment to Council policies in relation to Equal Opportunity, Customer Care and service delivery, and the ability to implement these policies in the workplace.
B	**Qualifications/Training/Certificates** **Degree in ICT/Computer Science or related field OR comparable experience within Digital, Data and Technology.** ▪ Professional certifications (e.g. CISSP, CISM, Microsoft certifications) ▪ For example, Azure AD, Defender, Intune, Conditional Access, Purview, and related technologies.

C	**Skills, knowledge and experience** ▪ Significant experience working as a security architect or senior security specialist in a complex organisation to enact cyber security controls. ▪ Strong experience designing secure solutions in Microsoft 365 and Azure environments. ▪ Experience working with legacy systems and designing pragmatic, risk-based security controls. ▪ Experience delivering or assuring security for cloud migrations, identity modernisation, and Zero Trust initiatives. ▪ Experience working with public-sector frameworks such as CAF, PSN, PCI DSS. ▪ Deep understanding of security architecture, threat modelling, and secure-by-design principles. ▪ Strong knowledge of Microsoft security technologies and modern identity approaches. ▪ Understanding of network security, endpoint security, encryption, and secure integration patterns. ▪ Ability to balance ideal security models with the realities of legacy technology and operational constraints. ▪ Excellent analytical, problem-solving, and communication skills. ▪ Pragmatic, risk-aware, and able to design secure solutions in imperfect environments. ▪ Collaborative and able to build trust with technical and non-technical colleagues. ▪ Influencing skills, including the ability to influence members, senior officers, partners and suppliers. ▪ Strong understanding of public sector governance, risk, procurement and regulatory frameworks. ▪ Evidence of continuous professional development in relation to security architecture and best practice. ▪ Strong commitment to equality, diversity, and inclusion as it applies to the role.

OUR VALUES AND BEHAVIOURS

Our values and behaviours underpin everything we do.
They guide our interactions with residents, businesses, visitors, partners and each other.
They are also a measure of how well we've done.

	Our Values & Behaviours

D	**PUTTING COMMUNITIES FIRST** • We put local people at the heart of decision making in everything we do. • We seek to include and involve: all voices matter. • We provide quality services that are responsive, effective and efficient. The following examples are indicators of effective behaviour: • I actively involve and include the communities that I serve in my work. • I shall reflect the views of the communities in my daily work. • I shall improve the service I provide through seeking feedback from others. Our residents will feel that: • I have been included • I can see how my views have been taken into account • I can see improvements and developments based on my input
E	**RESPECT** • We listen to everyone and value the personal experiences of people in our communities and of each other. • We adopt a fair and involving approach regardless of any way in which an individual is different to us. The following examples are indicators of effective behaviour: • I adapt my approach to take account of all differences and cultures in the community and with colleagues. • I ensure I am equitable and fair by including those who are quiet or may not be able to represent themselves. • I communicate in a way that is respectful, encourages involvement and meets people's needs. Our residents will feel that: • I feel my culture and background are respected. • I have confidence that action is being taken. • I feel I am being treated fairly.
F	**INTEGRITY** • We act with openness, honesty, compassion, responsibility and humility.

	• We let people know what we are doing and communicate why and how decisions have been made. The following examples are indicators of effective behaviour: • I demonstrate empathy in my interactions with others. • I am honest and transparent about the decisions I take. • I follow through on the actions I say I will take and take ownership for communicating the outcome. Our residents will feel that: • I am told when something is not possible, and the reasons why are explained to me. • I feel my perspective is listened to and understood. • I feel my views are valued
G	**WORKING TOGETHER** We work together and in partnership with everyone that has an impact on the lives of our residents. • We want to understand, learn from each other and continually adapt. The following examples are indicators of effective behaviour: • I work with others to provide an effective service for residents, local communities and other departments within the Council. • I seek ways to work with other departments to deliver a seamless service and find opportunities to improve. • I seek out opportunities to learn from my colleagues and build on good practice. Our residents will feel that: • I can get my issue resolved without being passed around departments. • I find it easy to access the services that I need. • I feel the Council is open to new ideas.