

**Directorate:** Chief Executive's Department  
**Unit/Section:** Technology Division  
**Grade:** KR12  
**Responsible to:** ICT Compliance & Risk Manager

### **Purpose of the Job:**

The ICT Security Lead works to ensure that The Authority's ICT infrastructure and data is secure to industry standard baselines and compliance/regulatory requirements. The ICT Security Lead drives security initiatives and control implementation to build The Authority's security architecture, advising on implementation of security standards within technical projects.

The role provides subject matter expertise on cyber security for The Authority and works closely with key suppliers to ensure performance of KCC's Information Security Management System, highlighting key risks and appropriate controls formally at a senior level. The position will formally investigate security incidents and apply appropriate knowledge to take action to reduce impact, including leading on retrieval of information to support internal investigations and breaches of ICT Policy.

### **Main duties and responsibilities:**

- Provide subject matter expertise within KCC for Cyber Security to provide authoritative advice and guidance on the application and operation of all types of security initiative and control.
- Provide expertise and extensive knowledge in specialist areas, working in partnership with senior management team in order to plan for emerging changes, strategies or initiatives within the organisation. Provide professional advice on complex and politically sensitive queries. Attend meetings, instigate and direct the resolution process, in order to inform decisions and prepare briefing notes for Members and senior officers.
- Monitor, manage and actively improve The Authority's Information Security Management System. Work with technology partners and suppliers to assure that security controls are working effectively and highlight emerging risks and appropriate controls to Senior Leadership in alignment with industry trends and best practice.
- Assure that security operations activity and security monitoring capabilities are appropriately actioning alerts to mitigate incidents, and handle active security incidents to work with and advise operational teams on actions to contain and reduce impact of the incident. Conduct investigation, analysis and review following breaches of security controls, and manages security incidents. Prepare recommendations for appropriate control improvements, involving other professionals as required.
- Provide information to prepare support technical compliance submissions for The Authority, including liaising with technical staff to implement required remediation work to ensure continued compliance to security standards as new and increased vulnerabilities

are recognised. Ensure a pragmatic approach is taken given the risks involved in implementing the remediation or accepting the risk.

- Identify threats to the confidentiality, integrity, availability, accountability and relevant compliance of ICT systems. Conduct risk and vulnerability assessments of business applications and computer installations in the light of these threats and recommends appropriate action to management. Manage and provide security advice and approval for software and applications on corporate devices.
- Monitor technical information to identify cyber security vulnerabilities and threats, and work with key suppliers to analyse data and take appropriate action to minimise risk to The Authority's ICT in terms of confidentiality, integrity and availability. Conduct security control reviews in well-defined areas. Assess security of information and infrastructure components. Investigate and assess risks of network attacks and recommend remedial action.
- Apply industry standards, compliance/legislative requirements and advice from key partners such as the NCSC to develop and implement The Authority's technical security architecture to embed and advise on 'secure by design' into systems under development in alignment with the Technology Strategy. This includes ensuring that appropriate controls are included at the early stage of the project, advising where necessary of deficiencies and required remedial actions to be taken.
- With discretion and whilst following instruction from responsible parties, extract technical logs and information for the purpose of investigations on KCC staff activity ensuring the integrity of the data and that the information is fully understood by the teams responsible for the investigations.

Footnote: This job description is provided to assist the job holder to know what their main duties are. It may be amended from time to time without change to the level of responsibility appropriate to the grade of post.

## Kent County Council

### Person Specification: *ICT Security Lead*

The following outlines the criteria for this post. Applicants who have a disability and who meet the criteria will be shortlisted.

Applicants should describe in their application how they meet these criteria.

	<b>CRITERIA</b>
<b>QUALIFICATIONS</b>	<ul style="list-style-type: none"><li>• Educated to degree level in an ICT related field and/or meets experience requirements</li><li>• Hold either CISA, CISSP or equivalent professional qualifications in IT/Cyber Security</li></ul>
<b>EXPERIENCE</b>	<ul style="list-style-type: none"><li>• Proven experience in a cyber security related role or in a directly relevant field of ICT</li><li>• Experience of ICT incident management processes</li><li>• Experience in Information Security Governance</li><li>• Experience of working in or with the Public Sector</li></ul>
<b>SKILLS AND ABILITIES</b>	<ul style="list-style-type: none"><li>• Operations Management – Proficient with methods, techniques and tools for planning, organising, resourcing, directing, coordinating and monitoring ongoing (non-project) activities</li><li>• Conceptual Thinking - Acquiring understanding of the underlying issues in complex problems or situations by correctly relating these to simpler or better understood concepts, models or previous experiences</li><li>• Oral and Written Expression - Communicating effectively by word of mouth and in writing</li></ul>
<b>KNOWLEDGE</b>	<ul style="list-style-type: none"><li>• Structured Reviews – Proficient in methods and techniques for structured reviews, including reviews of technical diagrams, test plans, business cases and any other key deliverables</li><li>• Business Characteristics – Proficient in the functional structure of businesses and other organisations; their mission, objectives, strategies and critical success factors. Knowledge of organisational culture</li><li>• Business Environment - Familiar with the business environment relating to own sphere of work (KCC and suppliers, customers and partners), in particular those aspects of the business which the team is to support</li><li>• Technical Field – Expert in theory, current practice and latest developments in the field of cyber security and general technology</li><li>• Corporate Industry and Professional Standards – Expert in specific standards associated with the role</li></ul>
<b>KENT VALUES AND CULTURAL ATTRIBUTES</b>	<b>Kent Values:</b> <ul style="list-style-type: none"><li>• We are <b>brave</b>. We do the right thing, we accept and offer challenge</li><li>• We are <b>curious</b> to innovate and improve</li><li>• We are <b>compassionate</b>, understanding and respectful to all</li><li>• We are <b>strong together</b> by sharing knowledge</li><li>• We are all <b>responsible</b> for the difference we make</li></ul>

	<p>Our values enable us to build a culture that is:</p> <p><b>Flexible/agile</b> - willing to take (calculated) risks and want people that are flexible and agile</p> <p><b>Curious</b> - constantly learning and evolving</p> <p><b>Compassionate and Inclusive</b> - compassionate, understanding and respectful to all</p> <p><b>Working Together</b> - building and delivering for the best interests of Kent</p> <p><b>Empowering</b> - Our people take accountability for their decisions and actions</p> <p><b>Externally Focused</b> - Residents, families and communities at the heart of decision making</p>
--	--

# Organisational Responsibilities

All corporate directors, directors and senior managers have an explicit responsibility to deliver the collective agenda of the Council. These are fundamental elements of their role not an addition and are summarised as follows:

## Whole Council

- Seek to improve the lives of all residents in Kent and economy of Kent
- Act as corporate parent to the Council's looked after children
- Take an active role in promoting and ensuring the Council's responsibilities for safeguarding are met.
- Understand, communicate and contribute to the delivery of KCC's strategic aims
- Meet statutory obligations and promote and ensure compliance with policies and procedures and the Council's Code of Conduct (Kent Code).
- Advise elected members and support the democratic process
- Promote the Council brand and enhance the overall reputation of the Council
- Understand and monitor the measures of performance, including customer insight, which define successful outcomes for KCC services
- Maintain and ensure a relentless focus on the customer
- Act to support the Council-wide need to deliver services within budget, thereby avoiding an overspend that could damage the financial viability of the Council
- Overcome professional and service silos to achieve the County Council's objectives.

## Integration of Services

- Focus resources where they have the biggest impact
- Deliver services that are flexible and adaptable
- Integrate services within KCC and work with partner agencies to ensure a seamless customer experience
- Fully and inclusively engage all staff in the delivery of services, demonstrating the Council's leadership values and competencies.

## Embedding Commissioning and Engaging relevant markets

- Establish an outcome focused organisation
- Meet the financial regulations and standing orders of KCC
- Challenge the status quo and engage with the market to constantly improve
- Ensure all services are delivered effectively and efficiently
- Proactively and continuously seek to improve service delivery
- Proactively manage risk to avoid inertia whilst not exposing the Council to needless and avoidable challenge or loss

## **Managing Change**

- Understand and support the Authority's overall change agenda
- Deliver required outcomes of service specific change on time and to budget
- Understand the quality of staff, support their development, nurture those with talent
- Identify the skills for the future and the level of staff through robust workforce planning
- Identify and deal with underperformance.
- Deliver to agreed budget and income targets.