

## CYBERSECURITY COMPLIANCE OFFICER

## Job Description

|                      |                             |                               |     |
|----------------------|-----------------------------|-------------------------------|-----|
| <b>Directorate:</b>  | Resources                   |                               |     |
| <b>Service:</b>      | Digital Commissioning       |                               |     |
| <b>Location:</b>     | County Hall                 |                               |     |
| <b>Salary range:</b> | Grade 10                    | <b>Grade:</b>                 | 10  |
| <b>Reports to:</b>   | Risk and Governance Manager | <b>Staff responsible for:</b> | 1-2 |

## Job purpose and scope

The purpose of the Cybersecurity Compliance Officer is to ensure that the organisation is compliant with Council and Government policy and guidance and to ensure Digital have the correct controls in place to address changes in the cyber threat landscape to manage and minimise risks associated with cyber..

To provide professional advice on all aspects of Information & Cyber Security and Assurance to colleagues across Digital Services and the Council. To be responsible for the creation and operation of an Information Assurance framework, to meet evolving business needs and changing industry standards. To manage ICT staff and partners engaged in Information Security and Assurance activities.

## Performance Indicators

- Responsible for continuous monitor and analysis of cyber threats to ensure the organisation stays ahead of emerging risks, providing actionable intelligence that informs security decisions, improves defences, and supports incident response.
- Quality of advice/service against legal, safety and best practice standards
- Achievement of relevant service targets
- Adherence to internal/external quality standards if applicable
- Adherence to policies and procedures

## CYBERSECURITY COMPLIANCE OFFICER

### Accountabilities/Responsibilities

- Proactively identify any need for specialist, external expertise regarding best practice in Security and Information Assurance, and to procure appropriate services where necessary and then monitor their effectiveness and compliance.
- Provide specific expertise and advice on government standards and industry best practice relating to Information Security to the Council. Ensure that compliance with these standards is embedded into all aspects of service delivery by providing direction and guidance to colleagues.
- Work with senior customers to provide strategic input to the development and operation of a framework of policies, procedures and meetings to ensure that security and information assurance requirements are fulfilled across LCC and its customer groups.
- Maintain continuous awareness and evaluate the impact of the evolving cyber threat landscape and emerging risk
- Work with the Security Architect for the creation and update of security roadmap.
- Communicate Information Security and Assurance matters internally and externally to key stakeholders, including LCC Senior Management, legal professionals, security regulators and internal/external auditors.
- Guide and liaise with colleagues across Digital Services on matters related to Security by Design and Security Operations.
- Work closely with LCC Information Governance and Data Protection colleagues to ensure a joined-up approach.
- Keep up to date with emerging Information Technology.
- Effectively establish and manage stake-holder relationships
- Due to the changing nature of the business, this job description serves as a framework to outline the main areas of responsibility. It is not intended to be either prescriptive or exhaustive and will inevitably change. You are expected to be flexible and may be required to operate in different areas of work/carry out different duties as required.

## CYBERSECURITY COMPLIANCE OFFICER

**Other**

- **Equal Opportunities**  
We are committed to achieving equal opportunities in the way we deliver services to the community and in our employment arrangements. We expect all employees to understand and promote this policy in their work.
  - **Health and safety**  
All employees have a responsibility for their own health and safety and that of others when carrying out their duties and must help us to apply our general statement of health and safety policy.
  - **Customer Focused**  
We put our customers' needs and expectations at the heart of all that we do. We expect our employees to have a full understanding of those needs and expectations so that we can provide high quality, appropriate services at all times.
  - **Safeguarding Commitment**  
We are committed to protecting and promoting the welfare of children, young people and vulnerable adults.
- ☐ **Skills Pledge**  
We are committed to developing the skills of our workforce. All employees will be supported to work towards a level 2 qualification in literacy and numeracy if they do not have one already.

## CYBERSECURITY COMPLIANCE OFFICER

### Our Values

**We expect all our employees to demonstrate and promote our values:**

- **Supportive**  
We are supportive of our customers and colleagues, recognising their contributions and making the best of their strengths to enable our communities to flourish.
- **Innovative**  
We deliver the best services we possibly can, always looking for creative ways to do things better, putting the customer at the heart of our thinking, and being ambitious and focused on how we can deliver the best services now and in the future.
- **Respectful**  
We treat colleagues, customers and partners with respect, listening to their views, empathising and valuing their diverse needs and perspectives, to be fair, open and honest in all that we do.
- **Collaborative**  
We listen to, engage with, learn from and work with colleagues, partners and customers to help achieve the best outcomes for everyone.

### Person Specification

All the following requirements are essential unless otherwise indicated by \*

Your ability to meet the job requirements will initially be assessed by the information provided on your application but further assessment will be undertaken at interview and, in some cases, by using other types of assessment(s).

### Qualifications

- Professional and/or academic level qualification (e.g. CISM / CISSP, certified with ISO 27001 lead implementer or lead auditor, ITIL Service Management Qualification, Cyber Security, Information Systems, Security or related degree) or equivalent experience, OR
- Substantial vocational experience in a relevant technical, scientific, specialised or operational field

### Experience

## CYBERSECURITY COMPLIANCE OFFICER

- Client-facing, with current experience delivering security consultancy specifically ISO27001, PCI, CLAS etc.
- Current experience encompassing Information Security Management (policy, procedures, controls, awareness, ISO 27001, Risk Management, Information Security, Information Governance, Certification, GAP analysis, compliance and risk assessment backgrounds).
- Experience of researching emerging cyber threats, vulnerabilities and attacker techniques, and assessing their relevance to organisational environments.
- Local Government experience\*
- Experience of NHS Data Security and Protection Toolkit, PSN, PCI-DSS and Compliance\*
- Managing staff\*
- Vulnerability management\*
- 

### Essential knowledge, skills & abilities

- Ability to analyse and interpret complex problems
- Comprehensive knowledge of Information Security Management Systems with the ability to scope, design and implement such systems
- Excellent written and verbal communication skills
- Ability to deal with highly complex and high-risk problems across the diverse range of IT security threats
- Ability to translate highly complex technical matters into user friendly language
- Ability to lead with innovative ideas, and proactively create and drive a 'business benefits' approach

### Other essential requirements

- Commitment to equality and diversity.
- Commitment to health and safety.
- Display the LCC values and behaviours at all times and actively promote them in others.
-