Job description

Job title Head of Cyber Security

- Grade: PO10
- Reports to: AD – Information and Digital Governance
- Direct reports: 5
- Your team: Cyber Security
- Service area: Information and Digital Governance/Islington Digital Services
- Directorate: Resources

Special requirements of the post
Workstyle: Desk-based worker (Lower presence, one day a week minimum) • Colleagues who are not usually client or customer-facing and can mostly work anywhere with the right technology. Regular on-site activities are required such as team events and collaboration that are more productive face to face
This post requires a Basic DBS check and BPSS check
This post is subject to the council's declaration of interest procedure
This post is designated as politically restricted

Our mission

Islington is a place rich with diversity and culture. As a council our sense of purpose couldn't be clearer: we serve. It's in the logo. We are committed to challenging inequality in the borough and as one of the largest employers we know that to look after the place and the planet, we have to look after our people. **Together we can change the future**.

To do this, everyone who works at Islington Council lives by a set of values which guide us in everything that we do: collaborative, ambitious, resourceful, and empowering. They spell out 'CARE', which is what we think public service is all about.

Overview of the role

The Head of Cyber Security will set the strategic direction for the council for cyber security develops policies and procedures, oversees governance and compliance, and acts as key advisor on cybersecurity matters. The postholder will lead the Cyber Security team to drive and embed the highest standards of cyber security to protect the council's technology, ensuring compliance with PSN, CAF, and NCSC guidance.

The Head of Cyber Security will be responsible for researching and implementing cyber defence best practices, auditing compliance with policies and legislation. Providing expert advice to directors and the Corporate Management team (CMT) on emerging on cyber-risk risks and opportunities. The postholder will manage incidents and investigations and foster a culture of accountability and risk management.

Key responsibilities

Please list each key responsibility of the role (Maximum of 10-12 bullet points):

- Lead and motivate a team of Cyber Security subject matter experts setting clear objectives and professional standards. Empower staff to promote continuous improvement in the organisations approach to cyber security.
- Provide expert direction to directors, the SIRO, CMT, and Councillors to foster a culture of cyber security by design and data protection ethics across the organisation, ensuring robust cyber risk management through comprehensive reports, updates, and briefings.
- Create and maintain the cyber security strategy, roadmap and target operating model ensuring that this is aligned with council objectives. Develop and maintain metrics and KPIs to provide a clear narrative on the council's security posture.
- Own the council's cyber security policies, ensuring their development, implementation, regular review, and continuous improvement to reflect emerging threats, technologies, and regulatory requirements. Champion and embed security by design principles throughout all organisational processes and projects, supporting responsible technology adoption and innovation from initial conception through to delivery and ongoing operation. Ensure that all policies and standards set a clear framework for secure practices and are effectively communicated, understood, and enforced across the organisation.
- Lead on cyber security investigations ensuring alignment with NCSC incident response guidance including conducting post incident reviews. Coordinate relevant personnel to respond to any incidents so that risks are contained and remedied as soon as possible. Liaise with external organisations such as the NCSC and third parties where appropriate.
- Lead the Security Operations capability providing leadership and oversight ensuring robust monitoring, detection and response to cyber threats across all council systems and networks. Develop and maintain effective incident response protocols in line with NCSC guidance, coordinate the Security Operations team to proactively identify, investigate, and mitigate security incidents, and drive continuous improvement through regular reviews and adoption of best practices.
- Collaborate with technical teams, suppliers, and external partners to enhance threat intelligence and operational resilience, ensuring the council's security posture remains adaptive to emerging risks and technologies.

- Own and continually improve incident response playbooks. Ensure that these are regularly tested and updated with lessons learned to support the organisations business continuity and disaster recovery preparedness.
- Oversee internal and external audits, penetration testing, resilience exercises including red/purple team exercises. Provide reports on outcomes to senior leadership ensuring continual improvement and learning.
- Oversee compliance with and submissions for accreditations such as CAF, PSN, DSPT, PCI DSS and Cyber Essentials +. Track remediations ensuring timely completion to achieve required certifications.
- Lead comprehensive communication campaigns and innovative training programmes to embed a cyber conscious culture. Ensure training is tailored to all levels, from front-line staff to senior leaders and measure its impact. Leverage modern digital learning tools and champion continuous learning that regularly tests and assesses the council's awareness.
- Any additional duties consistent with the grade and level of responsibility of this position, for which the holder possesses the required experience and/or training.

Budget responsibilities

Responsible for all cyber security contracts with a budget of up to £200,000.

Compliance

Ensure adherence to legal, regulatory, and policy requirements under UK GDPR, Health and Safety, Employee Code of Conduct and in your area of expertise by identifying opportunities and risks, and escalating issues as necessary.

Person specification

Your application form needs to demonstrate how you fulfil the role's requirements. It is essential to address the criteria, as this will be used to evaluate your suitability for the position.

Essential and desirable criteria

Essential: the basic requirements that must be met for someone to be considered for a particular job. These criteria are mandatory and cannot be negotiated. Essential criteria directly impact the core qualifications or skills necessary to perform the job effectively.

Desirable: the additional qualities, skills, or qualifications that would be advantageous for a candidate to possess but are not mandatory. Not meeting them does not automatically disqualify someone from consideration for the job. This also allows candidates who do not possess certain desirable criteria the opportunity to explain how their other knowledge, experience and skills relate to these and what they may be in the process of doing or willing to do to achieve these.

Knowledge, experience, and skills

Point	Criteria description	Essential/desirable
1	Educated to degree level or commensurate business qualifications or and demonstrable work delivered to degree level standard, ideally to include cybersecurity accreditations including CISSP or equivalent profession qualification.	Essential
2	Expert knowledge and experience of strategic Security Operations Centre development and management in large complex organisations, ideally including substantial public sector delivery organisations.	Essential
3	As a subject matter expert in a highly complex professional field, excellent skills in the design and implementation of very complex IT environments across multiple services and technology layers.	Essential
4	Experience of responding, managing and mitigating cyber security risks across large and complex technology environments and platforms, including ensuring effective security models are designed and implemented across Enterprise level complex IT architectures.	Essential
5	Extensive experience of working at a strategic level with key stakeholders, navigating top level organisational politics with evidence of managing by influence to achieve successful outcomes to complex business problems.	Essential
6	Demonstrate calm, empathetic decision-making under pressure, ensuring discretion and confidentiality while handling sensitive information during investigations.	Essential
7	Considerable experience of building, leading, and motivating individuals and teams including staff recruitment and performance management (both direct reports and matrix aligned staff).	Essential

Point	Criteria description	Essential/desirable
8	Demonstrate strong influencing skills, showing drive, tenacity, resilience and sound judgement in advising and providing expert direction at Board level leadership around technology acquisition, development and implementation.	Essential
9	Knowledge of and proven ability to work to standards including ITIL, Prince 2, ISO 27001, ISO 27002 Data Protection Act and other legal and regulatory frameworks relevant to the management of a public sector ICT service.	Essential
10	Knowledge and experience of technologies used to protect and secure the perimeter of the organisation including firewalls and intrusion detection systems.	Essential
11	Ability to understand, assimilate, create and maintain effective documentation detailing precise, complex technical and operational information to a variety of audiences including other technical experts, senior officers and elected members.	Essential
12	Ability to focus on quality and results whilst driving the delivery of mission critical systems and services in a pressurised environment with the ability to confidently support, assure and challenge with ease whilst maintaining good working relationships.	Essential

Our accreditations

Our accreditations include: The Mayor’s Good Work Standard, Disability Confident Employer, London Living Wage Employer, Stonewall Diversity Champion, and Employer with Heart.