JOB DESCRIPTION

POST TITLE: Cybersecurity Engineer

GRADE: PO4

DEPARTMENT: Resources

DIVISION/UNIT: IDS/Commercial and Risk

REPORTS TO: Head of Cyber Security

MANAGES/SUPERVISES: N/A

PRIMARY JOB FUNCTION

1. To research, interpret, disseminate and implement best practice in cyber defence and network security including ISO27001, NCSC (the National Centre for Cyber Security) guidance and Public Services Network instructions.
2. To verify and audit compliance with Council policy, relevant codes of practice and appropriate legislation including the Data Protection Act in all matters relating to network security.
3. To provide expert domain support for incidents and investigations into breaches of Council policy, relevant codes of practice and appropriate legislation, liaising with the relevant authorities and monitoring our platforms for information risk issues.

DUTIES AND RESPONSIBILITIES

Research and advice

4. To research, review, investigate, develop and implement new technologies to maintain and enhance the technical security of the Council's network in line with business requirements, best practice and regulatory requirements.
5. To engage with suppliers, advisers and regulators to review, upgrade and enhance the security of the Council's network; ensuring compliance with mandatory codes of connection.
6. To advise the ICT Architect, Business Architects, Solutions Architects and the Technical Design Authority on security architecture, network security, reviewing the network security implications of technical designs and

implementations.

7. To work closely with programme and project managers advising on projects that have technical security risks.

Compliance

8. To implement and maintain the daily operation and implementation of IT cyber security across the Council's networks.
9. To monitor, verify and audit compliance with best practice in network security including ISO27001, NCSC guidance and Public Services Network instructions on the Council's network.
10. To enforce and improve existing standards across the council, reacting to national standards and where applicable write these new standards in to council policy.
11. To ensure the technical protection and security of data and technology assets.
12. Define and write the policy for 3rd party connection standards to the council network and systems. Review and augment the policy regularly.
13. To use and be responsible for security event management systems, intrusion prevention systems, vulnerability scanning tools and end point security systems.
14. To demonstrate compliance to Internal Audit and external regulators, leading on relevant audits and technical aspects of the Council's Public Services Network Code of Connection, NHS Information Governance Toolkit and Payment Card Industry (PCI) submissions.
15. To provide extracts and reports required by customers using existing tools, such as Solar Monitor, Bluecoat Reporter, Exchange logs / Powershell queries, Proofpoint and Nessus.
16. To provide expert guidance on security patching and upgrades for council applications, databases and interfaces, updating the councils patch Management Policy regularly and ensuring that IDS staff are aware of their responsibilities.

Investigations

17. To provide expert domain knowledge for dealing with security incidents, trigger investigations and provide reports to the Head of Cyber Security.
18. To have an exceptional level of discretion and confidentiality to undertake investigations involving access to highly sensitive, confidential material which may be damaging to the reputation of the council, citizens or employees.
19. To provide expert domain knowledge into the response on the technical aspects of data security incidents, breaches of security controls, investigating events and reporting on impacts, ensuring evidence is secured to support further actions by the relevant authorities.

20. To support the Head of Cyber Security in any technical aspects of investigations, ensuring evidence is secured to support further actions by the relevant authorities.
21. To represent the Council in presenting the findings of technical investigations at briefings, hearing and in court.
22. To be able to withstand cross examination by counsel during tribunals and possible prosecutions. Be able to effectively deliver the results of any investigation to the examining bench or panel.

Business Continuity

23. To support the implementation of the council's strategy and policy for technical disaster recovery. Provide technical advice to the council on disaster recovery and business continuity requirements.
24. To provide guidance on practical business continuity of core infrastructure and systems during planned maintenance (e.g. during monthly service shutdowns).

Staff

25. To support and encourage staff to be creative, flexible and committed to providing solutions to the needs of the business and to relate to their customers in a clear, friendly and prompt manner.
26. To occasionally supervise apprentices, trainees, staff undertaking job shadowing, secondments and other forms of work experience.

Meetings

27. To participate in meetings with colleagues, customers and suppliers including team meetings and service review meetings.
28. To represent Islington Council in external forums.

Other

29. To undertake other duties commensurate to the grade of the post.

ADDITIONAL:

- The service operates from 8am to 5.30pm so you will be required to work as directed within these hours; and you may be required to carry out essential maintenance work on our monthly "Shutdown Sunday" or at other times out of hours.
- Occasional lifting and transporting of moderately heavy objects, such as servers, computers and peripherals.
- Occasional inspection of IT equipment, including servers, switches, cabling and storage.
- To use and assist others in the use of information technology systems to carry

out duties in the most efficient and effective manner.

- To achieve agreed service outcomes and outputs, and personal appraisal targets, as agreed by the line manager.
- To undertake training and constructively take part in meetings, supervision, seminars and other events designed to improve communication and assist with the effective development of the post and post holder.
- The post holder is expected to be committed to the Council's core values of public service, quality, equality and empowerment and to demonstrate this commitment in the way they carry out their duties.
- Ensure all the services within the area(s) of responsibility are provided in accordance with the Council's commitment to high quality service provision to users.
- Ensure that duties are undertaken with due regard and compliance with the Data Protection Act and other legislation.
- Carry out duties and responsibilities in accordance with the Council's Health and Safety Policy and relevant Health and Safety legislation.
- At all times carrying out responsibilities/duties within the framework of the Council's Dignity for all Policy. (Equal Opportunities Policy).

Post holder Declaration

Name:	
Signed:	
Date:	

ISLINGTON

PERSON SPECIFICATION

The person specification is a picture of skills, knowledge and experience required to carry out the job. It has been used to draw up the advert and will also be used in the short-listing and interview process for this post.
You should demonstrate on your application form how you meet the following essential criteria.

Department: Resources	**Section: IDS/Commercial and Risk**
Post Title: Cybersecurity Engineer	**Grade: PO4**

	REQUIREMENTS	
	EDUCATION and EXPERIENCE	**A/I/T***
E1	Extensive experience of working as part of a multidisciplinary ICT team in a large ITIL aligned organisation in a regulated industry, ideally a local authority.	A/I
E2	Trained in and/or experienced in the operation at least two security vendor's software, hardware or services or holding a relevant and current professional ICT security qualification.	A/I
	KNOWLEDGE, SKILLS and ABILITY	
E3	Extensive knowledge of networking principles, practices and technologies and the ability to apply this knowledge in a practical environment to deliver high performance, reliable and secure services.	A/I
E4	Technologies used to protect and secure the perimeter of the organisation including firewalls and intrusion detection systems	A/I
E5	Ability to transfer fundamental knowledge and experience from one technology to other technologies to gain a rapid understanding of its operation.	A/I
E6	Ability to work in a high-pressure environment and make sound decisions in emergency situations while empathising with customers and responding sympathetically to circumstances.	A/I
E7	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.	A/I/T
E8	Knowledge of and proven ability to work to standards including ITIL, Prince 2, ISO 27001, ISO 27002 Data Protection Act, General Data Protection Regulations and other legal and regulatory frameworks relevant to the	A/I
E9	Excellent time management skills combined with prioritisation skills to balance conflicting and often high profile priorities.	A/I

E10	Ability to work regularly one Sunday a month for scheduled maintenance, upgrades and installations and occasionally in the evenings and at weekends for other maintenance, upgrades and installations that cannot be completed during the scheduled monthly shutdowns.	A/I
	COMMITMENT TO EQUAL OPPORTUNITIES	
E11	Ability to adhere to the Council's Dignity for All policy	A/I
	SPECIAL REQUIREMENTS	
E12	Be able to work from home or equivalent location to be within reasonable distance of Islington.	
E13	This role will require you to have a high level of discretion and confidentiality as investigations involve access to highly sensitive and confidential material.	A/I
E14	This role will require you to obtain a basic satisfactory clearance from the Disclosure and Barring Service previously known as the Criminal Records Bureau (CRB) Disclosure.	✓
E15	This role requires Baseline Personal Security Standard pre-employment checks.	✓
E= Essential D= Desirable		
***Assessed by: A= Application I= Interview T= Test**		