Role Profile

Job Title:	**Cyber Security Manager**
Location:	**Colindale (Hybrid)**
Department:	**Technology services**
Directorate:	**Strategy & Innovation**
Grade:	**Grade M**
Type of Working:	**Hybrid Working**
Reports to:	**Assistant Director, Resident Experience, Digital & Commercial**

1. Job Purpose:

The Cyber Security Manager will lead the Council's approach to safeguarding its technology assets, systems, and data against evolving cyber threats. This role is responsible for developing and implementing a robust cyber security strategy aligned with national standards and local government best practice. The postholder will oversee risk management, compliance, and incident response, ensuring the resilience of critical services and the protection of sensitive information.

Acting as the Council's subject matter expert, the Cyber Security Manager will drive a culture of security awareness across the organisation, provide strategic advice to senior leaders, and manage relationships with external partners to maintain a secure and trusted digital environment.

2. Key accountabilities:

The Cyber Security Manager will:

- Act as the strategic lead for cyber security across Barnet Council, safeguarding critical ICT infrastructure, sensitive resident data, and council services from cyber threats. This includes leading incident response, ensuring compliance with national standards, and embedding cyber resilience across all Council operations.
- Ensure all ICT systems and processes are secure in line with NCSC guidelines, while supporting service delivery for Council staff, residents, and businesses.
- Manage and develop the Council's cybersecurity framework, including governance and security systems delivered through outsourced partners and with inhouse teams.
- Monitor and ensure PSN compliance is maintained, including annual health checks, responding to security breaches, and ensuring appropriate reporting and remediation activities with service providers.
- Monitor and ensure PCI-DSS compliance is maintained, including quarterly ASV scans, annual audits, and submissions, while managing responses to data breaches and ensuring corrective actions.

- Collaborate with the ICT managers, Service Delivery Managers, digital and data transformation programmes and Enterprise Architects to embed cybersecurity by design within Council change governance.
- Play an active role in the Change Advisory Board (CAB) and provide leadership for the Councils Security Board, in regards cyber security
- Contribute to Council-wide and directorate initiatives by assessing impacts, implementing business priorities, and supporting corporate objectives to meet the needs of Barnet's citizens and businesses.

- Build and maintain effective working relationships with stakeholders internally (across departments) and externally (suppliers, government bodies, and agencies).

Key outputs of the role will be to:

- Lead the development and implementation of all security policies, processes, and standards to safeguard Council technology, information systems, and ICT eco systems.
- Ensure 3rd party compliance to council's security standards and the right governance processes are embedded and complied to when onboarding suppliers and throughout the contract lifecycle
- Provide technical oversight across SIEM, firewalls, endpoint protection, and identity/access management.
- Ensure secure configuration of cloud and hybrid environments (Microsoft 365, Azure), and oversee patch management, disaster recovery, and business continuity testing, throughout the Councils supply chain.
- Develop and apply a standard testing approach that prioritises user experience for all major initiatives, in regards cyber protection.
- Communicate security processes effectively to ensure compliance across all Council services.
- Monitor systems for risks, including data breaches and gaps in security mechanisms, and implement corrective measures.
- Design and deliver integrated security solutions covering people, processes, and technology.
- Ensure compliance with external standards and frameworks such as PCI-DSS, HSCN (N3), DSP Toolkit, PSN and Cyber Essentials Plus.
- Work with business units and outsourced service providers to maintain appropriate procedures and controls, ensuring regular scans are conducted and vulnerabilities remediated.
- Plan and implement security measures across all information systems and networks and review designs for new projects to ensure they are implemented based on NCSC guidelines and ISO27001.
- Review and assess the impact of key government and local government ICT strategies on the Council's information security standards and policies.
- Provide input to senior management on the design development and execution of ICT security strategies.
- Oversee and perform security scanning including – Internal Vulnerability scans, External penetration scans using tools such as Nessus, PCI-DSS, PSN, Cyber Essentials Plus.
- Assess information risks and ensure agreement of risk profiles with technology partners and service providers against the corporate risk register.
- Ensure that technology solutions are compliant with security standards.
- Investigate information and ICT security breaches and work with stakeholders to ensure that appropriate controls are put in place to prevent recurrence.

- Manage the Council ICT service providers to ensure passable scans, collating data at regular intervals, ensuring the organisation maintains a vulnerability management program and builds up the key evidence to demonstrate compliance.
- Monitor user awareness and training to ensure optimum understanding and use of ICT resource and good cyber control practices.
- Provide the corporate expertise in PCI-DSS and liaising with service units to ensure that all payment card handling is complaint.
- Work with the Information Governance Manager/Data protection Officer to develop information security policies and ensure they are implemented and communicated across all services.
- Attend project meetings to provide advice and ensure compliance when the organisation is implementing any project that might impact on the existing compliant status.
- Work with the Councils IT provider to prepare the annual compliance submissions and present to Managing Director and Senior Information Risk Owner (Siro) for sign off. Work with the relevant validation authorities to obtain accreditation/certification and acceptance of the Council's security controls.
- Manage the working relationships with internal colleagues / clients and gain feedback on a regular basis on customer expectations, particularly engaging with Corporate Directors and Senior Managers as appropriate
- Manage and maintain appropriate Stakeholder Management relationships with Internal and external service providers / suppliers and agencies to ensure delivery of services are in line with the Council's expectations
- Will involve line management duties as the Councils operating model evolves and develops, alongside transitions with the Councils current IT outsource provider

3. Financial Responsibilities:

Budget responsibility up to £100k but is also responsible for managing significant risk for the council and subsequent financial impact if correct mitigations are not in place. (£20m+)

4. Health and Safety Responsibilities:

As an employee of the London Borough of Barnet, you are required to:

- Abide by Barnet's health and safety policy and associated arrangements
- Complete mandatory health and safety training
- Follow safe systems of wok and use devices/guards provided for safety.
- Wear/use personal protection equipment were issued and instructed to do so, including lone working devices.
- Report any Accident/Incidents/Hazards.
- Take care of your own and other's safety, health and wellbeing

5. Promotion of Corporate Values

To ensure that customer care is maintained to the agreed standards according to the council's values. To ensure that a high level of confidentiality is maintained in all aspects of work. Our values:

Caring / **L**earning to Improve / **I**nclusive / **C**ollaboration

6. Flexibility

In order to deliver the service effectively, a degree of flexibility is needed and the postholder may be required to perform work not specifically referred to above. Such duties, however, will fall within the scope of the post, at the appropriate grade.

7. The Council's Commitment to Equality

To deliver the council's commitment to equality of opportunity in the provision of services. All staff are expected to promote equality in the workplace and in the services the council delivers.

PERSON SPECIFICATION

Job Title	**Cyber Security Manager**
Location:	**Colindale (Hybrid)**
Department:	
Directorate:	**Strategy & Innovation**
Grade:	**Grade L/M**
Type of Working	**Hybrid Working**
Reports to:	

Criteria	Essential/Desirable	Assessed by:
Professional Membership/Qualification		
A professional qualification in cyber security information management or other relevant area. Those working towards such a qualification would be considered.	Desirable	Application

Experience & Knowledge		
Proven experience in cyber security management within public sector or regulated environments or large-scale private company.	Essential	Application & Interview
Strong knowledge of NCSC guidance, PSN, PCI-DSS, GDPR, and Cyber Essentials Plus.	Essential	Application & Interview
Experience and knowledge in Microsoft Sentinel, Microsoft Defender, and Microsoft E5 security toolsets, including the application of Microsoft Copilot for Security	Essential	Application & Interview
A professional qualification in cyber security information management or other relevant area. Those working towards such a qualification would be considered.	Desirable	Application & Interview
Proven experience of balancing technical, commercial and other issues to deliver business advantage.	Desirable	Interview
Excellent organisational skills to effectively plan and handle workload with conflicting priorities as well as maintaining a balanced customer focus.	Desirable	Interview
Comprehensive knowledge and understanding of best practice modelling as it relate to Cyber Security management.	Essential	Interview
Skill & Ability		
Strong interpersonal skills to build a high degree of credibility and presence to negotiate, influence, inspire confidence and respect, to develop a network within and outside of the Council.	Essential	Interview
Comprehensive knowledge and understanding of best practice modelling as it relates to Cyber Security management.	Desirable	Interview

Strong analytical ability with attention to detail, specifically focusing on analysing and interpreting complex statistical data including trends and performance management data, with a view to producing accurate and meaningful reports.	Desirable	Interview
Clear and robust understanding of the technical, and legal aspects of Business Relationship policies and processes to ensure successful and robust interpretation and resolutions	Desirable	Interview
Ability to carry out duties outside normal working hours as may be necessary including response to emergency situations and the out of hours services.	Desirable	Interview
Ability to work efficiently and effectively in a demanding and pressurised environment	Desirable	Interview

independently and as part of a team to contribute to the broader ICT agenda.		
	Desirable	Interview
	Desirable	Interview
Values & Behaviours		
Caring		
Integrity- I work with candidates and colleagues in a way that builds trust.	Essential	Interview
Empathy- I say “thank you” and “well done” where appropriate, and take time to ‘check in’ to see if the people I work with are ok	Essential	Interview
Support- I support my colleagues to deliver excellent services. I focus on resolving any issues and capturing lessons learnt	Essential	Interview
Learning to Improve		
Insight- I regularly rely on evidence and professional standards to support my work and decision making.	Essential	Interview
Agile-I am fully empowered to act within the scope of my role	Essential	Interview
Growth Mindset- I take responsibility for my own personal development, growth and learning and support others with their learning and development where I can	Essential	Interview

Inclusive		
Personal Responsibility- I am curious about what is important to others around diversity. I reflect and act upon this curiosity to improve my own understanding	Essential	Interview
Engage with discomfort- I am open to and reflect on what makes me uncomfortable and use my engagement with others to challenge myself and constructively challenge others	Essential	Interview
Champion Diversity- I recognise the advantages and importance of equality, diversity and inclusion in delivering outcomes for residents, and take an active role to ensure they are implemented and integrated in everything I do.	Essential	Interview
Collaborative		
One Team- I actively and purposefully build my network of relationships with people across the Council and with partners. I proactively seek	Essential	Interview
feedback and evidence as a way of learning from and improving the way I work with others		
Accountable- I accept responsibility for my own actions and decisions, and demonstrate commitment to ensuring these align to what is best for Barnet	Essential	Interview
Outcomes Focused- I adapt my way of working to best suit the outcome we are trying to achieve within the scope of my role and professional standards	Essential	Interview