**Manchester City Council
Role Profile**

**Senior Cyber Security Analyst - Grade 8
ICT Service, Corporate Core Directorate
Reports to: Cyber Operations Platform Manager
Job Family: Technical**

Key Role Descriptors:

The role holder will undertake a lead consultant role on complex technical, procedural and legislative matters in a professional, customer focused, specialist technical service.

The role holder will lead and have accountability for the delivery of a range of technical projects, initiatives or work packages that comply with relevant legislation and help achieve the Council's corporate aims and objectives

The role holder will use their technical knowledge and expertise to develop, design and implement customer-focused solutions. They will continually identify and champion opportunities to deliver improvement.

Key Role Accountabilities:

Lead an innovative, forward thinking technical consultancy function for the assigned service area, ensuring that solutions are delivered in line with customer and legislative requirements. Dependent on the service area, this may include software / information technology support, engineering, surveying, curating or other specialist functions.

Lead on the delivery of work packages (using project management methodology where appropriate), ensuring compliance with organisational objectives, consistency in approach and compliance with appropriate internal and legislative guidelines.

Actively strive to achieve efficiencies in project, programme and maintenance service delivery and improvements in the quality of service.

Develop successful internal and external relationships and secure stakeholder commitment through negotiation and communications, both oral and written, to ensure work packages are delivered effectively and to customer requirements and agreed objectives. Work closely with contractors where required to ensure effective work package delivery.

Analyse and interpret legislation, presenting information and complex technical matters relating to the service area in a clear and concise manner to a range of stakeholders, orally and in writing. This will include identifying and addressing

complex issues and making informed recommendations on action needed to support key corporate objectives.

Represent the City Council as an expert witness at enquiries, tribunals and hearings or similar proceedings where appropriate.

Roles at this level may be required to manage a range of assigned resources, which may be human, financial or other, to ensure continuous improvement in service delivery. Staff management duties may be either through direct line management of a team (including appraisals, performance management and other duties) or through matrix management of a virtual team of officers.

Dependent on the service area, the roleholder may be required to work on a rota basis including out of hours as required to meet customer demand.

Demonstrate a personal commitment to continuous self development and service improvement.

Through personal example, open commitment and clear action, ensure diversity is positively valued, resulting in equal access and treatment in employment, service delivery and communications.

Where the role holder is disabled, every effort will be made to supply all necessary aids, adaptations or equipment to allow them to carry out all the duties of the role. If, however, a certain task proves to be unachievable, job redesign will be fully considered.

Role Portfolio:

Manchester City Council
Manchester City Council (MCC) supports a resident population of approx. 575,000 people and employs over 7300 staff & supports various external partnerships. The *Our Manchester Strategy - Forward to 2025* sets out how MCC will create a sustainable, equal and inclusive city. At the heart of these ambitions is the desire to achieve equality for all Manchester communities, recognising that for some communities this will mean more support is needed to reduce inequalities and improve outcomes.

The Council is split into Directorates: Adults' Services; Chief Executive's; Children's Services; Corporate Services; Growth and Development; Neighbourhoods; Population, Health and Wellbeing.

ICT & Digital Department
The vision of the ICT & Digital department is "a relentless drive towards digitally empowering better outcomes for the Council and its communities using inclusive, secure & connected technologies to underpin exemplary ICT & Digital service delivery."
The ICT & Digital department support Manchester City Council by providing technology, infrastructure, and digital services. These range from public facing websites to network operations and cloud services. ICT Portfolio and core functions include:

- **Digital Delivery & Business Partnering:** Lead and direct ICT for each of the Council directorates, ensuring the ICT Strategy is aligned to the delivery of the City's strategic priorities and enables services to deliver effectively. The Heads of Digital Delivery & Business Partnering are responsible and accountable for all new ICT & Digital related demand within the specific directorates for which they are responsible utilising teams of programme, project, and product managers to support the continuous delivery of transformational change.

- **Portfolio & Departmental Management Office (PDMO):** Ensures alignment of all ICT & Digital activity with strategic objectives, outcomes, and capacity to deliver, to enable benefit realisation and support continual service improvement. Provides governance standards across all ICT & Digital areas to allow proactive selection, prioritisation, and control of the complete portfolio of activity. Has overarching responsibility for all financial management, contracts and licensing that underpin effective transition and sustainable ICT & Digital service delivery.

- **ICT Operations:** Provides the core operational function of the ICT & Digital department. It is responsible for the following IT Infrastructure Library (ITIL) functions: Service Desk, IT Operation Management, Technical Management, Platform Management and Application Support Management. ICT Operations is at the forefront of ICT service delivery and is one of the most important elements that keeps the organisation running.

- **Cyber Security & Compliance:** Provides the operational security controls, security guidance, security assurance, cyber risk management, and compliance activities that support all products and platforms within the Council. Protects networks, devices, and data from unauthorised access or criminal use by the practice of ensuring confidentiality, integrity, and availability of information.
- **Enterprise Architecture (EA):** Provides a well-defined practice for conducting enterprise analysis, design, planning, and implementation for the successful development and execution of strategy. Enterprise Architecture reduces redundancy, complexity and information silos and business risks associated with ICT investments.

A high-level summary is provided below to add scale and context to the wide variety of services provided by the Council's ICT & Digital service that is also supported by an investment plan to deliver Digital Transformation across:
- 212 Office locations inc. 27 libraries
- Circa 8000 ICT users and 96 elected Councillors
- 200+ Line of Business Applications
- 1000+ Virtual Servers hosted across resilient Cloud and On-Prem Data Centres
- 10,000+ Laptops, PC's, and associated End User Devices
- 300 printers

Cyber Security and Compliance Team
The wider Cyber Security and Compliance Team provide the operational security controls, security guidance, security assurance and compliance activities that support all products and platforms within the Councils. Protecting networks, devices, and data from unauthorised access or criminal use by the practice of ensuring confidentiality, integrity, and availability of information. These services underpin all operational IT and digital services for the whole organisation that are consumed by our internal staff, external partners along with the customers, residents and visitors of Manchester.

Cyber Operations
The Cyber Operations team provide pro-active threat hunting capabilities along with security governance, assurance and compliance activities, create and manage policies and processes to ensure that all technology remains secure and compliant. Through continuous vulnerability scanning the Cyber team test all security layers are safe, secure and compliant against both our Internal Security Standards and Statutory Obligations whilst ensuring that all supporting hardware and software is current, capacity managed, and professionally documented and administered; either internally or by 3rd parties.

Typical security platforms / applications managed by the Cyber Operations team include (but not limited to):

- Firewalls
- DMZ
- Web Filtering
- Email Filtering
- Ransomware Protection
- Endpoint Detection and Response
- Security Incident and Event Monitoring (SIEM)
- Vulnerability Identification and Management
- OS and Application Security Patching

The role and experience of the Senior Cyber Security Analyst should include:

- A minimum of 5 years experience working in an IT Security Operations team with detailed knowledge of managing network, server, applications and end user computing in a complex environment.
- Familiarity with the concepts and operation of common security applications and tooling.
- Broad knowledge of Security and Cloud architecture principles
- Experience of security monitoring, alerting and service recovery in a pressurised and complex environment.
- Recent experience as a senior member of a multi-disciplinary team managing security (firewall / filtering / DMZ / Pen Testing / Vulnerability Management) and potential 3rd party teams.
- Accredited to a recognised Security qualification eg. CISSP, CCP, CCSP . The successful candidate must be willing to work towards obtaining a referenced qualification if not already achieved.
- Recent experience of providing high quality management reports; supported by transparent and factual data analysis; with the aim of demonstrating problems, opportunities for risk reduction and improvement across the service.
- Ability to perform Investigations and Forensics, provide Security Representation on Projects, to perform Threat Management and Vulnerability Assessments.
- A strong understanding of Prince2 (or equivalent project management methodology) and how projects should be transitioned into production and the rules and standards that govern this transition. Specifically, so that IT Security can confirm that projects / 3rd parties are delivering / testing standard Security layers / process with the required support documentation to run the service.
- Significant experience of IT Service Operations, and how an IT installation works across 24x7 and a high level of knowledge of ICT Security environments, risks and challenges
- Significant knowledge of the relevant legislative framework and professional standards both within the ICT and Security industry and in particular to a Local Authority.
- To work flexibly including out of hours and bank holidays as required to meet customer demand and potential incidents up-to a Major Incident.

Key Behaviours, Skills and Technical Requirements

- We are proud and passionate about Manchester
- We take time to listen and understand
- We 'own it' and we're not afraid to try new things
- We work together and trust each other
- We show that we value our differences and treat people fairly

Generic Skills

- **Communication Skills:** Is able to effectively transfer key and complex information to all levels of staff, adapting the style of communication as necessary and ensuring that this information is understood. Writes convincingly and clearly, succinctly and correctly, avoids the unnecessary use of jargon or complicated language; writes in a well-structured and logical way and structures information to meet the needs and understanding of the intended audience.
- **Analytical Skills:** Skills to analyse a wide range of data and other sources of information to break them down into component parts, patterns and relationships; probes for further understanding of problems and makes rational judgements from the available information and analysis demonstrating and understanding of how one issue may be part of a much larger system/issue. Ability to absorb, understand and quickly assimilate complex information and concepts and compare information from a number of different sources.
- **Planning and Organising:** Excellent time management skills, creating own work schedules, prioritising, preparing in advance and setting realistic timescales for own self and others. Has the ability to visualise a sequence of actions needed to achieve a specific goal and how to estimate the resources required.
- **Project Management:** Ability to identify, assess and manage risks to the success of the project.
- **Problem Solving and Decision Making:** Ability to formulate independently a range of options for new or unfamiliar situations and to select the appropriate course of action to produce a logical, practical and acceptable solution. An ability to make independent decisions of a relatively uniform nature.
- **Research & Intelligence:** Ability to conduct research using a variety of techniques, in order to gather evidence and evaluate intelligence, recording in compliance with documented standards and legislation.
- **ICT Skills:** Skills to configure appropriate areas of technical support in a large organisation. Skills to ensure the availability, integrity and search-ability of information through the application of formal data structures and protection measures.

Technical requirements (Role Specific)

- Qualified to BSc Computer Science/Cyber Degree or Accredited to a recognised Security qualification eg. CISSP, CCP, CCSP (Must be willing to work towards achieving if the qualification/accreditation is not held)
- Qualified to ITIL, with a strong practical understanding of how the core ITIL functions (CM / IM / PM / RM and Configuration Management) interface and interact to collectively support IT and the Business.