Job description

Job title: Cyber Security Manager

Department: Transformation and Change, Finance & Resources
Service: IT Service
Grade: J
Post reference number:

1 Job purpose

To provide expert organisation-wide cyber security management, support and advice in a complex IT environment, according to industry standard best practice. To provide high level expertise to large, complex IT projects and be the key escalation point for cyber security related issues.

To define, develop and deliver cyber security services across the Council, providing leadership and design expertise for cyber security across the IT Service. Ensure the Council has robust risk management, security operations, architecture and incident response in place to protect against cyber threats and data breaches.

2 Principal duties and responsibilities

1. Responsible for the development, implementation, delivery, and support of an enterprise cyber security function, aligned to the strategic requirements of the council to safeguard all Council systems and data.

2. Responsible for cyber security activities, ensuring that business continuity options are developed, maintained and tested. Ensuring user access and systems availability options are documented and according to the Council and IT Service business continuity plans.

3. Develop a close working relationship with both the SIRO and DPO, acting as subject matter expert. Advise NCC Corporate Leadership Team around current cyber security threat and required responsive posture, to represent NCC at national level, including at the governments National Cyber Security Centre (NCSC).

4. Lead and oversee security solutions/innovation and establish an enterprise security stance through strategy, policy, architecture, operational and training processes which ensures strong working practices, governance and compliance of cyber security across the Council.

5. Responsible for ensuring the council meets its cyber security certification and compliance aspirations, including Public Services Network (PSN), Cyber Essentials and Centre for Internet Security (CIS) frameworks.

6. Ensure IT security and cyber risk is documented, reviewed, analysed and reported to the wider council. Including the provision of key performance reports on service delivery against industry performance indicators and internal service level agreements on

weekly/monthly basis for relevant stakeholders as required.

7. Responsible for ensuring continuous service improvement through proactive and effective planning and design in conjunction with the Technical Design Authority, as co-chair.

8. To support forensic investigations for both civil and criminal cases, working with internal audit, government bodies and Nottinghamshire Police.

9. Lead on Learning and Development activities for the Council for Cyber Awareness.

10. Responsible for contributing to the procurement aspects of own area in order to meet project delivery timescales and effective fault resolution process for the department, including the use of contracting agency staff and of suppliers for software or application upgrades, patches or legislative changes as appropriate, to ensure an effective cyber security function.

11. Monitor the quality of service provided by the supporting teams and develop and implement any necessary changes to improve the delivery of service to customers. To develop standards for supporting core applications and ensure colleagues across the IT Service adheres to set processes and policies, ensuring systems are designed for high resilience and availability.

12. Regularly monitor the service request queues to maximise resource utilisation in the support of customer's issues and requests, provide regular updates to IT management on significant delays or service impacts and major incidents, supporting the Problem Manager in the performance of their duties.

13. To coach, mentor and develop the IT Security Analysts, Senior IT Security Analysts, and colleagues within the wider IT Service; ensuring that they are provided with the necessary tools, procedures and policies to enable them to deliver a high quality cyber security function.

14. Responsible for taking ownership of customer complaints and to investigate and ultimately resolve any complex incidents that are received at the Service Desk or that are passed from other IT Service Functions or IT Management.

15. To be proactive in the performance and systems monitoring, capacity planning and effective implementation of change management in support of core applications minimising impact on frontline services by ensuring high availability targets are met.

16. To maintain an awareness of major projects, planned developments and implementations, and so ensure they can be effectively communicated to and promoted to customers, and that the Cyber Security team have the necessary support, skills, and knowledge to underpin the overall service delivered to the front line customer services.

17. Carry out preventative maintenance and systems monitoring as defined by operating standards. Implementing new initiatives and future changes in service delivery, specifically related to corporate priority projects.

18. Deputise for senior leaders within the IT Service, as required.

19. To observe the regulations in the Data Protection Act 1998, Computer Misuse and Abuse Act 1990 and Regulation of Investigatory Powers (RIP) Act, and adhere to published and operational City Council ICT policies and procedures at all times. To ensure the

confidentiality, integrity and availability of corporate information assets and systems and, where appropriate, ensure preventative measures are undertaken to help mitigate the risk of a security incident occurring including reporting any security breaches or exceptions.

20. To work outside normal office hours as necessary and to participate in an out of hours on call rota if required.

21. To proactively build and develop a positive reputation for the IT Service by acting as an ambassador when dealing with other colleagues, customers and external partners and ensuring a positive customer and citizen focused approach at all times.

22. To proactively implement and embed IT service management good practice, such as the ITIL Framework, in all areas of work and ensure that positive contributions to all parts of the IT service management lifecycle are made at all times.

23. Contribute fully to the delivery of the Council's IT Strategy, and allied initiatives, which has a vision to provide a platform to develop and deliver consistently good quality, right first time, cost effective solutions and services that routinely surpass expectations and contribute to the successful transformation of Council service delivery and leads to improved outcomes for Nottingham's citizens.

3 All staff are expected to maintain high standards of customer care in the context of the City Council's Core Values, to uphold the Equality and Diversity Policy and Health and Safety standards and to participate in training activities necessary to their post.

4 This is not a complete statement of all duties and responsibilities of this post. The post holder may be required to carry out any other duties as directed by a supervising officer; the responsibility level of any other duties should not exceed those outlined above.

5 All staff must be aware of and adhere to the Council's Information Security Policy and IT Acceptable Use Policy. All employees have a responsibility to protect the Council's information and physical assets in accordance with these policies. Any breach of information security controls may result in disciplinary action being taken against them under the Council's disciplinary policy and may result in dismissal.

6 Numbers and grades of any staff supervised by the post holder:

1x Senior IT Security Analyst
1x IT Security Analyst

7 Post holder's immediate supervisor.

IT Infrastructure Manager

Prepared by/author: Alex Billing **Date:** April 2025

Job title: IT Infrastructure Manager

Note: This section should only be included in job descriptions issued to employees and should not be sent to all job applicants.

I understand and accept the job duties and responsibilities contained in this job description.

Signature: ..... **Date:** .....

Person specification

Job title: Cyber Security Manager

Department: Transformation and Change, Finance & Resources
Service: IT Service
Grade: J
Post reference number:

Areas of responsibility	Requirements	Measurement				
		P	A	T	I	D
Knowledge	Significant knowledge of methods and techniques for risk management, business impact analysis, countermeasures and contingency arrangements relating to serious disruption of IT service.		●	●	●	
	Knowledge of different security frameworks and standards such as NCSC CAF, Cyber Essentials, ISO 27001, etc.		●	●		
	Recognised training relevant to corporate IT Security environment support e.g. Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or equivalent.	●	●			●
	Understanding of customer service, ownership and feedback in the context of systems support, upgrades and change management.		●	●	●	
Experience	Experience in developing Cyber Security strategies, policies and procedures		●			
	Experience of working within IT security standards and data protection legislation.		●			
	Working experience in developing and training staff, developing processes, procedures and documentation.		●			
	Experience in methods and techniques for reporting progress and performance against targets, and planning and reporting progress against service requests and projects.		●		●	
	Experience in performance monitoring and analysis.		●			
	Significant experience in providing cyber security administration and support in a complex corporate IT environment.		●		●	
	Significant experience as a senior IT practitioner /		●			

	consultant in the field of IT application support and database administration management in large corporate organisation.					
	Understanding of cyber risks to organisations including potential security threats and data breaches.		●		●	
Skills / Abilities	Ability to produce clear written and verbal communications updates systems and databases accurately.		●	●	●	
	Ability to enhance technical skills through self development and formal training courses.		●			
	Ability to prioritise work and deliver results in a pressurised environment balancing conflicting demands to achieve acceptable outcomes.		●	●	●	
	Demonstrate ability to absorb a higher rate of change with an improved, measurable rate of success in delivering installation, deployment and on going operations and optimisation of IT projects and IT services such as major systems upgrades.		●		●	
Work to promote mutual respect and good relations	Awareness and understanding and commitment to the pursuit of equality of opportunity in terms of: • service delivery • employment practice		●		●	
Work Related Circumstances	To be willing to work outside of core working hours as required.		●			
	Willingness to comply with the City Council's non-smoking policy.		●			
	To be able to undertake a Disclosure & Baring Service (DBS) basic or full Checks with an outcome of satisfactory.	●				●
P: Pre-application	**A**: Application	**T**: Test	**I**: Interview	**D**: Documentary evidence		

Prepared by/author: Alex Billing **Date:** April 2025

Job title: IT Infrastructure Manager