Grading
Job Description and Employee Specification

Job title: Cyber Security Specialist	**Service area:** Outcomes
Post number:	**Division:** Technology & Communications
Grade: 10	**Section/team:** Infrastructure Technology

Overall purpose of job:

Support the Technical Delivery Specialist and the operational Infrastructure Technology teams to provide a secure, high-quality client and network infrastructure for the organisation and its partners.

The post-holder is responsible for providing assurance and oversight of the organisation's cyber security posture, setting direction, standards and expectations, and ensuring that appropriate technical, procedural and compliance controls are in place and operating effectively.

Post holders will be expected to be flexible in undertaking the duties and responsibilities attached to their post and may be asked to perform other duties, which reasonably correspond to the general character of the post and are commensurate with its level of responsibility.

Main responsibilities:

1. Monitor and analyse the council's IT and cyber security environment and activities, and oversee the response to security incidents, breaches and alerts, ensuring appropriate remediation and mitigation actions are progressed.
2. Support the development and implementation of the council's cyber security strategy, policies, standards, and procedures, in line with the national and local frameworks and best practices.
3. Ensure regular security assessments, audits and testing of the IT infrastructure are undertaken, including network, server, storage, backup and cloud solutions, and that vulnerabilities or gaps are identified, owned and addressed.
4. Support the design, configuration and maintenance of cyber security tools and systems, providing assurance that controls are effective and appropriately managed.
5. Provide guidance and advice to the infrastructure, business and innovation teams to contribute to drive continuous improvement in the organisation's cyber security capabilities and maturity.
6. Research and evaluate new and emerging cyber security threats, technologies, and solutions, and advise on risk, priorities and appropriate actions.

7. Ensure compliance with relevant cyber security legislation, regulations and standards, working closely with Information Governance colleagues to align cyber security controls with data protection requirements.
8. Work closely with the Technical Delivery Specialist and the Cloud Technical Specialist to provide assurance over the security and compliance of the council's cloud environment and services.
9. Support IT infrastructure projects and services, ensuring that cyber security requirements and risks are identified, assessed and appropriately managed throughout the project lifecycle.
10. Provide assurance and governance oversight for the development, maintenance and testing of IT business continuity and disaster recovery plans, ensuring that findings and actions are tracked and addressed.
11. Support the development and maintenance of business continuity and disaster recovery plans, providing assurance through testing and review.
12. Support the management of the IT infrastructure asset lifecycle and ensure security upgrades and patches are planned and delivered as needed.
13. Support the change and release management tasks ensuring adequate risk assessment and scheduling of technical changes and releases.
14. Support the delivery of the council's aims and objectives and represent the department at relevant local and regional forums and networks.
15. Provide senior oversight and strategic direction during major cyber security incidents, acting as the key escalation point and ensuring effective coordination and response.

Knowledge, skills and experience:

Knowledge & Skills

- Holds a professional qualification in a related subject area or relevant experience.
- Significant knowledge and experience of IT and cyber security principles, practices, and technologies, and the best practices and guidelines of relevant authorities and standards, with a focus on governance, assurance, compliance and risk management
- Significant knowledge and experience of IT and cyber security risk management, assessment, and mitigation, and the ability to assure and challenge technical approaches to cyber security and resilience.
- Understanding of network hardware and protection systems that provide defence in depth (e.g. firewalls, DDoS and intrusion prevention), sufficient to assess effectiveness and provide assurance.
- Knowledge and experience of technology compliance, legislation, and good practice.
- Political sensitivity, understanding and awareness.
- Excellent communication skills & interpersonal skills that inspire trust, encourage collaborative working and co-development.
- Ability to research, present and explain complex and technical issues to a wide range of audiences and sectors.
- Excellent leadership skills with the ability to foster a positive and motivated organisational culture.

- Excellent analytical and problem-solving skills.
- Influencing, negotiating and presentation skills.
- Ability to apply strategic and operational decision making.
- Ability to write and present reports, briefing notes and decision records.
- IT literate, with the ability to use and interrogate a variety of systems.
- Excellent time management skills, with the ability to work to tight deadlines and constantly changing priorities.
- Resilient and tenacious.
- Positive role model.
- Flexible approach to working arrangements.
- Ability to transport self around North Lincolnshire in a timely manner.

Experience

- Experience of providing senior guidance, assurance and guidance to operational teams, and supporting the delivery of IT and cyber security projects and services.
- Experience of overseeing IT and cyber security audits, assessments, and testing, and ensuring remediation and improvement actions are identified and progressed.
- Experience of researching and evaluating new technologies and innovations related to IT and cyber security and making recommendations to support the continuous improvement and transformation of the IT infrastructure.
- Change management experience.

Creativity and innovation:

- Maintain an innovative and responsive approach to the management of resources, having regard to the need for economy, efficiency, and effectiveness.
- Managing and motivating staff.
- Dealing with urgent operational matters, outside of normal working hours as required to protect the ongoing interests of the council and residents and/or communities etc.
- Regularly defines, develops, and reviews operational working practices within range of functional area.
- Apply creativity and innovation to develop governance approaches, assurance frameworks and improvement initiatives in response to complex cyber security and technology challenges.
- Deals with diverse non-routine, planned and unplanned service issues and, using judgement, responds creatively to customer requirements for which there may be no precedent.
- Provides authoritative and risk-based advice on cyber security and compliance matters to varied audiences, often at short notice.
- Resolve conflicting situations by personal intervention through consultation, negotiation, and mediation.
- Embrace and champion new ways of working including agile, flexible working.

Contacts and relationships:

The post holder will regularly deal with a range of complex operational matters, which will have significant implications on the service, the council, and the people of North Lincolnshire

- Technical Delivery Specialist – to discuss security related issues and planning – regular basis.
- Cloud Technical Specialist - to discuss security related issues and planning - regular basis.
- Information Governance leads and Senior Leadership – to provide advice, assurance and reporting on cyber security, risk and compliance – regular basis.
- Team members – to provide direction, assurance and professional guidance on cyber security matters – regular basis.
- Operational staff - to discuss security risks, compliance requirements and assurance outcomes – regular basis.
- Professional networks/government departments/regulators/other council`s – to discuss technical issues and/or operational practices – occasionally.
- Staff across the Operational Services area - consultation to identify and programme workload and discuss variations and pressures where applicable - weekly.
- Elected members/Cabinet – contact on complaints, service delivery and technical issues in the absence of the Technical Delivery Specialist – occasionally.
- Members of the public and local businesses - to deal with queries and corporate complaints on service delivery issues – infrequent.
- Peer Groups/External organisations – Frequently represents the council by attending national and regional groups, forming standards and representing the council's and local government's interests in IT and Cyber Security matters.

Decision making:

- Makes decisions relating to the security of posture of the authority alongside the Senior Information Risk Owner.
- Acts as a point of escalation and is trusted by the Senior Information Risk Owner as an expert advisor on cyber security risk and assurance matters.
- Evaluates and advises the correct course of action to take in the event of large impact IT and cyber security problems and incidents to minimise the consequences and impact to the services provided by the council.
- Determine the appropriate course of action and escalation in response to cyber security incidents to ensure effective resolution.
- Makes decisions linked to the development of all programmes of works.
- Decisions to ensure compliance across areas of responsibility.
- Investigation and resolution of complaints and appeals.
- Ensuring the welfare, health and safety of self and staff in areas of responsibility.
- Make recommendations for establishing the strategic direction of the council's cyber security services within Infrastructure Technology.

Responsibility for resources:

Financial resources:

- None

Physical resources:

- Laptop - £850
- Smart phone - £150
- Office based 100%
- Agile working is in place.

WORK ENVIRONMENT

Work demands:

- Work is largely operational, however, there will be strategic requirements to deal with that will impact on operational work.
- The workload to be undertaken is neither routine nor regular and fluctuates in terms of volume and nature and by its nature it cannot follow an established routine, given the requirements of the public, Town and Parish Councils, Council Officers, Elected Members and outside bodies.
- The postholder will provide oversight and assurance across technical teams, who may have conflicting priorities and deadlines.
- The work requires the management of complex, frequently changing and conflicting priorities.
- A high level of customer contact in a demand led environment necessitates prompt responses. Deadlines are usually very tight and timescales for completion of tasks short.
- The majority of the work is statutory, contractual or politically sensitive.
- The post has significant autonomy in structuring the working day requiring high levels of self-discipline and time management skills.
- A changing government agenda as well as emerging local need and technological and legislative change will require involvement in decision making processes at short notice. This may also require an immediate team re-focus and interruption to any normal programme of work, with involvement in crises management, both internally and with partners. Swift directional change may well result and will require collaborative re-contracting of work programmes with colleagues and partners.
- Unforeseen project and technical problems that require immediate action and attention, which can require out of normal contracted hours working.
- Demands of managing operational services across multiple areas in order to ensure services continue to operate effectively.
- Deliver to internal and external deadlines.
- Constant challenge to maximise use of the council's resources.
- Need to keep up to date with local, regional and national policy agendas.
- Responds to emergency situations (including out of hours), providing senior escalation, coordination and assurance where required.

Physical demands:

- None

Working conditions:

- Office based.
- Agile working is in place.

Work context:

- Minimal risk.

Grading
Job Description and Employee Specification

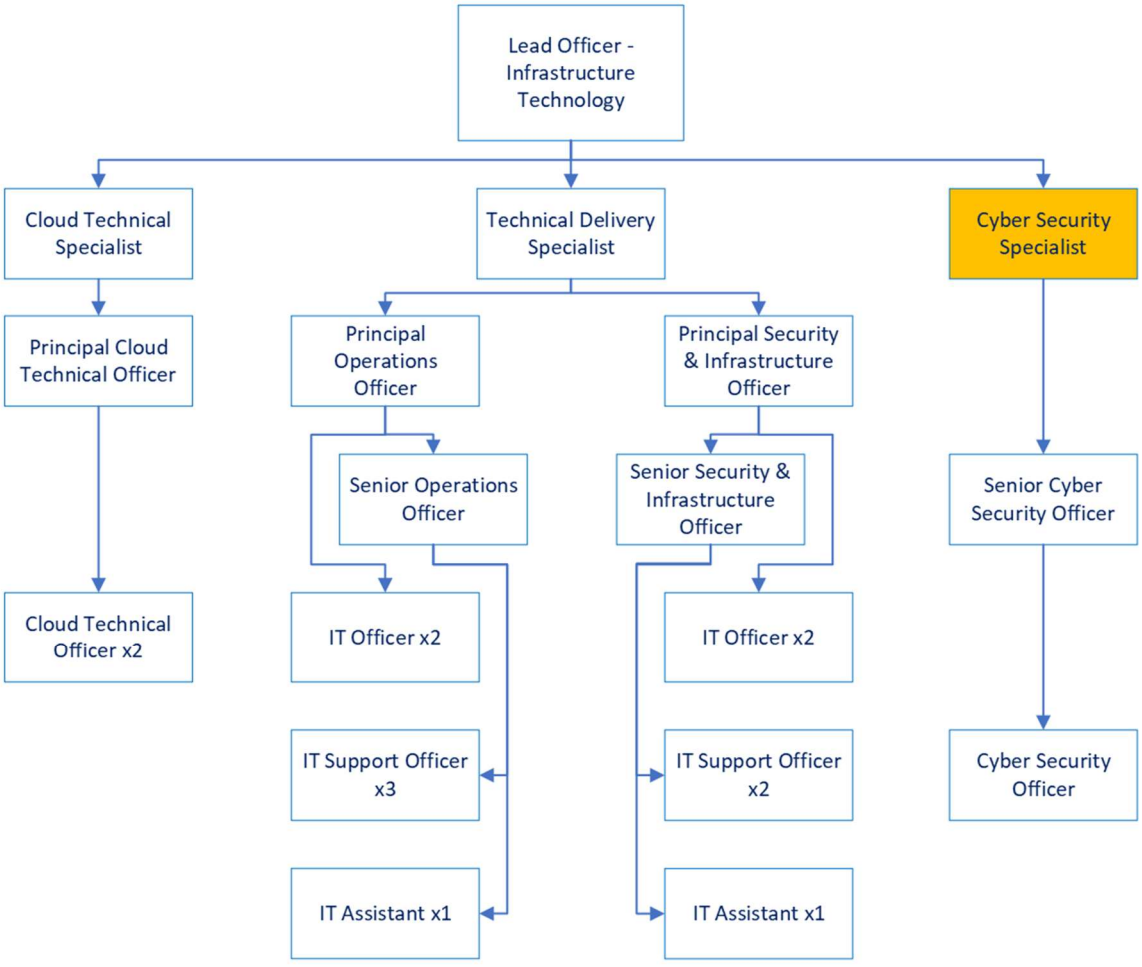
Position in organisation:

Indicate how many staff the post is directly accountable for: 2

Are posts in more than one location? Yes ☐ No ☐
Is this at the same site? Are the posts managed highly mobile? Highly mobile.

Is the supervision/management shared with another post in the structure?
Yes ☐ No X

Please indicate which post(s)



Job Description Version Control	
Date evaluated	3.6.26
Date updated	18.5.26
Updated by (manager name)	Mark Grimbleby
Checked by (HR name)	Jo Parker

Grading

Job Description and Employee Specification

ESSENTIAL CRITERIA	ASSESSED THROUGH:
Knowledge, Skills and Experience	**Application form (follow up at interview)**
• Significant knowledge and experience of IT and cyber security principles, practices, and technologies, and the best practices and guidelines of relevant authorities and standards, with a focus on governance, assurance, compliance and risk management. • Significant knowledge and experience of IT and cyber security risk management, assessment, and mitigation, and the ability to assure and challenge technical approaches to cyber security and resilience. • Understanding of network hardware and protection systems that provide defence in depth (e.g. firewalls, DDoS and intrusion prevention), sufficient to assess effectiveness and provide assurance. • Maintain a wide-ranging appreciation of current ICT issues, legislation, trends and market changes. • Knowledge and experience of technology compliance, legislation, and good practice. • Political sensitivity, understanding and awareness. • Excellent communication skills & interpersonal skills that inspire trust, encourage collaborative working and co-development. • Experience of providing senior guidance, assurance and challenge to operational teams, and supporting the delivery of IT and cyber security projects and services. • Experience of overseeing IT and cyber security audits, assessments, and testing, and ensuring remediation and improvement actions are identified and progressed. • Experience of researching and evaluating new technologies and innovations related to IT and cyber security and making recommendations to support the continuous improvement and transformation of the IT infrastructure. • Change management experience.	
Knowledge, Skills and Experience	**Interview**
• Ability to research, present and explain complex and technical issues to a wide range of audiences and sectors. • Excellent leadership skills with the ability to foster a positive and motivated organisational culture. • Excellent analytical and problem-solving skills. • Influencing, negotiating and presentation skills. • Ability to apply strategic and operational decision making. • Ability to write and present reports, briefing notes and decision records. • IT literate, with the ability to use and interrogate a variety of systems. • Excellent time management skills, with the ability to work to tight deadlines and constantly changing priorities. • Resilient and tenacious. • Positive role model.	
Education, Training and Qualifications	**Original documents**
• Holds a professional qualification in a related subject area or relevant experience.	
Working Arrangements	**Interview**

- Flexible approach to working arrangements.
- Ability to transport self around North Lincolnshire in a timely manner.

DESIRABLE CRITERIA	ASSESSED THROUGH:
Knowledge, Skills and Experience	**Application form (follow up at interview)**
•	
Knowledge, Skills and Experience	**Interview**
•	
Education, Training and Qualifications	**Original documents**
•	
Working Arrangements	**Interview**
•	

THE POST IS SUBJECT TO:	
Disclosure of convictions under the Rehabilitation of Offenders (Exemption) Act 1974	
Yes ☐	**No** ☐
Political restriction	
Yes ☐	**No** ☐
The ability to speak fluent English under the Immigration Act 2016	
Yes ☐	**No** ☐

- Version Control

Author	HR Policy Team
Status	V0.1
Date approved	19 September 2012
Last updated	21 December 2021