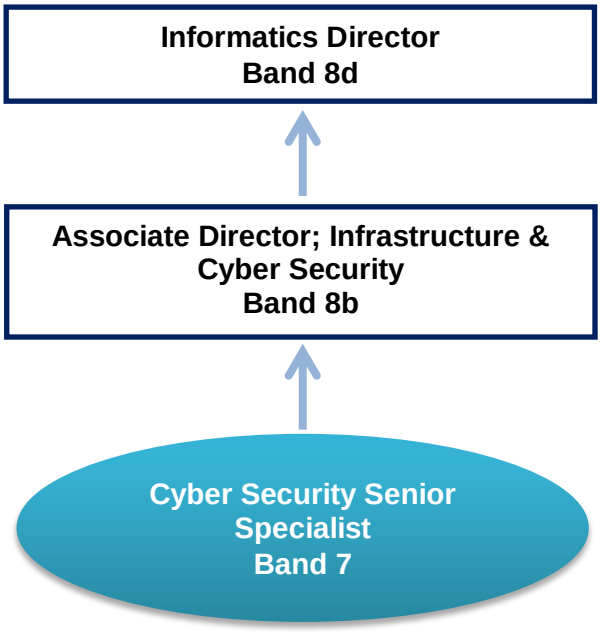
NHS
Countess of Chester Hospital
NHS Foundation Trust

Welcome to the Countess of Chester

Cyber Security Senior Specialist Band 7



Your opportunity

Job summary

The Post holder will be the Trust expert in Cyber Security and have responsibility for the effective implementation of the Cyber Security agenda across the Trust, as such, acting as a Lead Specialist for around 300 systems, covering approximately 4,500 end users. They will be required to monitor Cyber Security Systems, respond to Cyber Incidents and contribute to the development of policy, processes and procedures to reduce the likelihood of a Cyber Security incident.

As a senior member of the ICT team, they will undertake audit and risk assessments, monitoring of Cyber Security Systems and work with third parties to review compliance with best practice.

You will act as an escalation point for Cyber Security incidents and provide specialist advice and knowledge to support our ICT services and work with the Associate Director; Infrastructure & Cyber Security to assist in the development of Cyber Security Training packages for the team and organisation wide. This is increasingly important as digital services become a critical dependency in healthcare, the availability of those services is essential and therefore a culture of Cyber Security awareness needs to be engrained throughout the organisation.

You will be required to adhere to a Cyber Security professional code of conduct and keep up to date with legislation and national policies, as well as assessing security advisories from third parties.

The list below is to outline the main duties involved; however, this is subject to change and will vary within the given role. We ask all employees to be flexible in their role, to always ensure we are delivering Safe, Kind and Effective care.

The list below is to outline the main duties involved; however, this is subject to change and will vary within the given role. We ask all employees to be flexible in their role, to always ensure we are delivering Safe, Kind and Effective care.

Cyber security responsibilities

1. Monitor the changes in global cyber security threats and continually react to those threats. Implement appropriate checks and controls to protect the Information Assets held and managed by the organisation

2. Identify and address any potential and actual cyber security vulnerabilities in infrastructure and applications.

3. Ensure all ICT services are protected from malware and other emerging threats.

4. Continually assess options for the ongoing improvements in Cyber Security services, controls and procedures to maintain effective Cyber Security defences as the threat vector changes.

5. Develop Cyber Security procedures based on best practice, advice, and guidelines

6. Plan, organise and coordinate digital asset and system patching, in conjunction with critical health care services and other stakeholders within ICT, which may require a re-focus of activities, in order to deliver outcomes.

7. Review the security risks associated with all infrastructure components and supporting systems and services as related to users, processes and systems.

8. Assist in Architecture-certifying new applications from a cyber-security perspective.

9. Be a member of the National Cyber Security Centre (NCSC), proactively assess and act on device provided by the NCSC.

10. Provide technical advice, which will often be highly complex, in the development of business cases as directed by the Associate Director; Infrastructure & Cyber Security.

11. Provide cyber advice and support to ICT professionals and users of the ICT services.

12. Work closely with the Information Governance team to act as a source of expert technical advice in respect of information governance requirements relating to cyber security.

13. Work closely with the Informatics department being a subject matter expert for security considerations for third party device forms, DPIA & FOI enquires.

Education, development and improvement responsibilities

14. Lead in the implementation of national policies, local policies and proposals for service changes across the Trust, as directed by the Associate Director; Infrastructure & Cyber Security.

15. Undertake evaluation and redevelop where necessary the procedures within the Cyber Security service area. These redevelopments may impact on all service areas within the Information Department and throughout the organisation.

16. Propose changes to improve the functionality and effectiveness of Cyber Security systems as new threats and technology advances dictate.

17. Technically assure the solution and ensure changes are implemented as seamlessly as possible and that appropriate training is provided to the ICT teams for ongoing support.

18. Assist the Associate Director; Infrastructure & Cyber Security in achieving relevant Cyber Security certifications.

19. Ensure Information Resources are protected by effective Cyber Security controls in line with relevant NHS strategies and industry standards.

20. Responsible for the management and accuracy of an asset database that holds an inventory of Cyber Security services.

21. Develop ICT staff in Cyber Security skills and competencies.

22. Perform audits and vulnerability assessments on the digital assets.

23. Work with key stakeholders in ICT to ensure that compliance is retained and that, where this is not possible, appropriate risks are recorded and financial profiles and risk registers are updated.

24. Adapt, design Cyber Security Systems to ensure compliance with Cyber Security standards.

25. Responsible for introducing, adapting and improving Cyber Security Systems, proposing changes and making appropriate recommendations.

26. Ensure all Cyber security logs are monitored, kept up to date and acted upon, working closely with the wider ICT teams.

27. Adhere to the departmental electronic filing structures and contribute to the establishment and review of standards for the use of electronic filing across the Directorate.

28. Ensure reports are created on cyber security matters as directed by the Associate Director; Infrastructure & Cyber Security, both ad-hoc and agreed Key Performance Indicators (KPIs).

29. Assess the security impact and implications of incidents and events and report as appropriate.

30. Comply with relevant legislation in relation to General Data Protection Regulation (GDPR), Governance, Caldicott principles, and confidentiality, Human Rights Act, Freedom of Information Act etc. and the latest E-policies.

31. Create reports on Cyber Security systems where required and as directed by the Associate Director; Infrastructure & Cyber Security, both ad-hoc and agreed Key Performance Indicators (KPIs).

32. Identify key cyber security equipment and hold an accurate up to date list of hardware, firmware and software revisions.

33. Ensure equipment maintained by third parties is repaired and secured in accordance with agreed SLAs.

34. Undertake vulnerability scanning and surveys of network security systems.

35. Ensure technical refresh requirements in respect to Cyber security are submitted to the Associate Director; Infrastructure & Cyber Security on an annual basis. All equipment and software must have end of life dates recorded so long-term capital refresh planning can take these into account and ensure timely replacement of equipment and software.

36. Escalate reliability issues to the Associate Director; Infrastructure & Cyber Security. Ensure all organisational Cyber Security systems have up to date Systems Operating Procedures (SOPs) and Secure System Policies (SSPs).

37. Advise on the technical requirements in terms of Cyber Security on procurement of digital systems.

38. Ensure effective disaster recovery plans and evidence of testing are in place for services provided under the remit of ICT Services.

39. Provide a post Project quality assurance check and liaise with necessary Directorate staff on any security issues.

40. Conduct research and evaluation to identify and validate any proposed security technologies, both established and emerging as directed by the Associate Director; Infrastructure & Cyber Security.

41. Research and propose options to mitigate Cyber Security Vulnerabilities.

42. Ensure effective testing processes are undertaken for new hardware and software for Cyber security systems to improve and enhance the service, working closely with the ICT departments

that utilise these services.

Leadership responsibilities

43. Assist the Associate Director; Infrastructure & Cyber Security in ensuring technical compliance with the Network and Information System Directive (NIS-D)

44. Assist the Associate Director; Infrastructure & Cyber Security and the Head of Infrastructure in the annual review of maintenance contracts.

45. The post holder may be required to participate in activities regionally/cross organisation, in collaboration with individuals from other organisations, in order to support services and ensure effective use of Information and Communications Technologies informed by cyber security standards.

Communication responsibilities

46. Provide and receive complex, and highly complex, sensitive information relating to Cyber Security and the safe operation of the organisation's ICT systems.

47. Prepare reports based on Cyber Security incident statistics and organisational compliance with Cyber Security targets.

48. Assist in the Coordination of Cyber Security incident responses at organisational level.

49. Provide advice and coach staff in the secure and effective use of telephony and data networks and related ICT technology.

50. Work closely with internal teams, suppliers, maintenance contractors and distributors to maintain Cyber Security systems as appropriate.

51. Assist in the development and content of the Cyber Security pages on the Trust Intranet including publication of Key Performance Indicators.

52. Develop and maintain strong working relationships with all members of the ICT and Information Governance departments.

53. Liaise with Clinical and Business Managers, Departmental Managers, Switchboard staff, Information Managers and all users of ICT throughout the organisation.

Team responsibilities

54. Deliver formal and informal cyber security and awareness presentations to groups of staff – both internally and externally.

55. Act as a mentor to junior staff and coordinate work where appropriate.

56. Required to supervise work placements and allocate work for Contractors and junior staff where appropriate, relating to Cyber Security activities.

57. Responsible for authorising and procurement of technical tools and licensing that support cyber security assurance activity.

58. Responsible for shaping the annual capital plan and revenue for cyber security spend.

59. Assist the Associate Director; Infrastructure & Cyber Security in ensuring the wider ICT team perform to acceptable standards in relation to Cyber Security.

60. Required to participate in Divisional out of hours, on-call arrangements, as and when required.

61. All employees of the Trust always have the responsibility to comply with the Trusts Infection Prevention and Control policies and procedures. Strict adherence to effective hand hygiene is essential. All employees of the Trust have a responsibility for their own health and wellbeing, to inform their manager and seek timely support via the Trust's Occupational Health and Wellbeing department.

62. You have a responsibility to respond to any safeguarding children or adult concerns that you encounter in your everyday duties. You must report any concerns as appropriate to your immediate and the relevant safeguarding lead within the Trust.

Person specification

	Essential	Desirable
Qualification	• Educated to Degree Level in Cyber Security, or equivalent experience. • Cyber security qualifications or equivalent experience.	• Professional qualification/certification or membership in cyber security, for example membership of one or more of the following ISC2, BCS, CREST, CISSP qualification, ITIL Foundation qualification - MCSE/A
Knowledge and experience	• COMPTIA or equivalent level of work experience and knowledge • Detailed working knowledge of Desktop and Server or network security • Detailed knowledge of requirements for Cyber Essentials Plus CE+ • Detailed understanding of the Network Information and Information Systems Directive (NIS-D) • Good understanding of Cyber Security best practices, standards, certifications, and terminology. • Relevant experience working in Cyber Security, using relevant industry standard Security products and tools. • Evidence of Cyber Security or other relevant work outside formal training or employment (voluntary, research, academia, social media etc.) • Working with Security Information and Event Management (SIEM) and Vulnerability scanning solutions.	• Application of Cyber Security in a healthcare environment. • In-depth knowledge of one or more specialist areas such as compliance, penetration testing, or incident response. • Membership of professional body, e.g. BCS • Development of training packages. • Experience of ICT service provision in a health care setting. • Delivery of training to technical and non-technical staff. • Report writing. • Procedure development.
Skills and abilities	• Excellent communication and interpersonal when dealing with highly technical and highly • Complex information to a wide range of stakeholders. • Ability to quickly understand and apply new technologies.	• Thorough understanding of ICT and its application to healthcare

	Essential	Desirable
	• Ability to develop and maintain effective working relationships across multi-functional teams, in particular how to engage with users (technical and non-technical) in defining requirements and implementing solutions. • Ability to motivate, build and promote team working • Demonstrate significant levels of discretion, including problem solving, and maintain a 'can do' approach • Ability to work on own initiative, plan and organise own workload, and deliver projects with minimal support. • Sound judgement, decision making and organisational skills, with the ability to concentrate to significant levels on a frequent basis • Excellent technical and keyboard skills. • Requirement to analyse and manipulate data. • Ability to execute vulnerability scans and understand and present results. • Excellent letter, report and documentation writing skills along with presentation skills • Able to evaluate and assist in selection of best practice security tools • Ability to undertake Root Cause Analysis of security incidents • Significant keyboard skills and application use. • Able to adapt to change and keep up with new technologies using own initiative and discretion. • Ability to work within Change Management guidelines (ITIL). • Ability to identify and embrace change	

	Essential	Desirable
	in the drive towards continuous improvement	

Occupational health

	What you need	Conducted by	Essential
Health screening	Paper documentation and health assessment	Occupational health nurse	Yes
Maintenance staff immunity required	Hepatitis A	Occupational health nurse	Yes, vaccination recommended
Please note that the above may vary dependent on job role and risk assessments. Should you need further clarification please contact the Occupational Health Department on 01244 365045			

Our culture

Our vision

We will improve the lives of our community and provide excellence in health and care, through partnership and innovation.

Our values

Our Trust values and behaviours guide the way we do things. Our values are:

- **Safe**: Avoiding harm and reducing risk to all
- **Kind**: Considerate and non-judgemental
- **Effective**: Consistently maximising resources to deliver excellent and reliable care.

Our behaviours

We expect our staff to demonstrate the following behaviours: