SINGLE CORPORATE SERVICES

Digital

Job title:	Cyber Security Specialist	***To be completed by HR*** *Job Reference Number 2022/026*
Reporting to:	Technical Security Supervisor	
Accountable to:	Head of Service Delivery	
Pay Band:	6	

As part of the Single Corporate Service, this role provides a service across both Isle of Wight NHS Trust and Portsmouth Hospitals University NHS Trust.

The intention for the existing primary work locations to remain unchanged as there is no desire to change base locations unnecessarily. However, as the single corporate service will be delivered across both organisations, individuals may be required to undertake business travel from time to time. The staff mobility local agreement will apply.

For our leaders managing staff across multi-site locations, they will need to be visible and provide in person leadership. The arrangements and frequency will be agreed locally.

Job purpose

The Cyber Security Specialist will work as Technical lead to help manage cyber security compliance across the Trusts Digital Infrastructure and applications, reducing our Threat Exposure Score and minimising the attack surface across.

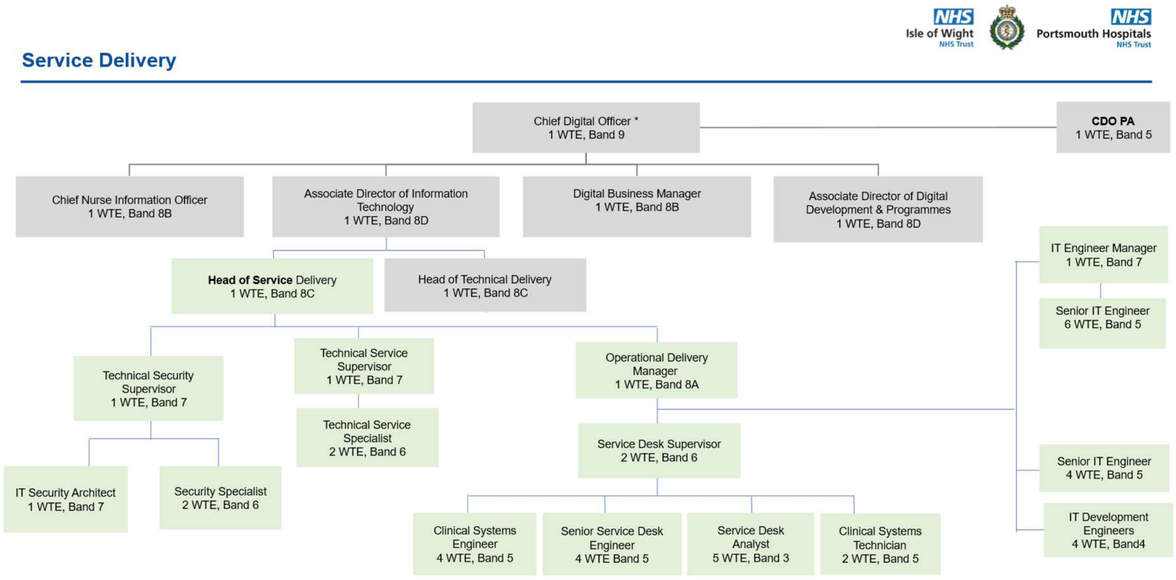
The post will liaise across Desktop, Applications, Systems and Network Teams to ensure all colleagues are kept updated and take the requisite actions to remediate threats to maintain security and integrity of Trust systems

Job summary

- To monitor privilege account usage working with the relevant engineers to ensure security requirements are met i.e. concept of least privilege, - separation of admin accounts and day-to-day accounts etc.
- To proactively monitor the Digital estate using the cyber tools available to identify potential threats, vulnerabilities and indicators of compromise. Then acting on the highly complex information in a suitable manner as required to allow The Trust to respond to and mitigate risk.
- Work with the relevant teams to ensure that all systems, (including mobile devices, PCs, Servers and network devices etc), are patched to recommended levels, applying security fixes and configurations as recommended by NHS Digital CareCERT.
- To use the cyber tool set to undertake in house audits of the Digital estate and produce the required reports.
- To assist auditors and third party companies to undertake IT security audits. With a view to maintaining continuous improvement within the estate.

- To maintain continual professional development to stay up to date with changing technologies and complete any relevant training that comes with this position.

Organisational Chart


NHS Isle of Wight NHS Trust
NHS Portsmouth Hospitals NHS Trust
Service Delivery
Chief Digital Officer * 1 WTE, Band 9
CDO PA 1 WTE, Band 5
Chief Nurse Information Officer 1 WTE, Band 8B
Associate Director of Information Technology 1 WTE, Band 8D
Digital Business Manager 1 WTE, Band 8B
Associate Director of Digital Development & Programmes 1 WTE, Band 8D
Head of Service Delivery 1 WTE, Band 8C
Head of Technical Delivery 1 WTE, Band 8C
IT Engineer Manager 1 WTE, Band 7
Senior IT Engineer 6 WTE, Band 5
Technical Security Supervisor 1 WTE, Band 7
Technical Service Supervisor 1 WTE, Band 7
Technical Service Specialist 2 WTE, Band 6
Operational Delivery Manager 1 WTE, Band 8A
Service Desk Supervisor 2 WTE, Band 6
IT Security Architect 1 WTE, Band 7
Security Specialist 2 WTE, Band 6
Clinical Systems Engineer 4 WTE, Band 5
Senior Service Desk Engineer 4 WTE Band 5
Service Desk Analyst 5 WTE, Band 3
Clinical Systems Technician 2 WTE, Band 5
Senior IT Engineer 4 WTE, Band 5
IT Development Engineers 4 WTE, Band4

Specific Core Functions

- To administer the current and future cyber security toolset in line with best practice. This will require a high level of technical proficiency and a willingness to maintain continual professional development so The Trust can maintain cyber maturity in a changing landscape.
- To monitor NHSD Cyber Alerts (CareCerts) , NCSC and CVE to understand and keep abreast of the changing threat landscape. Help to build and deploy patches and to advise colleagues in Desktop, Systems and Networks Teams to ensure we our threat exposure is minimised at all time.
- To create reports to facilitate understanding and remediation actions as required using the highly complex data received from The Trusts cyber security solutions including The Trusts AV solution, vulnerability scanning solution, SIEM solution, threat protection solution, patching solution and firewalls.
- To work with 3rd party suppliers of existing and new systems to ensure security best practices are in place on all systems.
- To work within the ITIL framework for incident, problem and change management.

Key Responsibilities

Communication and Working Relationships

- The postholder is expected to present and communicate highly complex multi-stranded and sometimes contentious information about the security threat, our exposure and compliance levels and to prepare reports on serious breaches

Analytical and Judgement

- The postholder be required to analyse and respond in real time to emerging threat data from a variety of national government and corporate sources, review vulnerabilities in light of our exposure, operational and clinical needs, to make key decision on what action is taken and when.

- They will analyse and interpret complex facts or situations, requiring comparison and valuation of a range of options.
- The postholder will be required to investigate and respond to security incidents and to ensure the security and integrity of Trust Systems, corporate and patient data.
- They will be required to develop, structure and schedule plans and strategies which include a variety of complex programmes in line with the digitisation plan.
- They will be required to adapt and adjust plans depending on the requirements for the organisation and ensure that appropriate remediation's are in place and tracked in response to a continually evolving cyber security landscape.

Physical Skills

- Have advanced keyboard and computer skills in particular the use of function and other special keys and key combinations to control and program a range of computer equipment and network devices.

Patient Client Care

- The postholder will have occasional contact with patients and carers in a wide variety of situations (including mental health) during the course of their duties.

Policy and Service Development

- The postholder implements Digital policies and procedures for their own professional area.
- They are closely involved in the development and implementation of policy for Information systems, security and governance.
- They monitor and enforce policies that affect the security and integrity of the Trust's computer systems and network and ensure that legislation is not breached.

Financial Management

- Postholder will be responsible for installation, configuration and maintenance of a range of cyber security systems.
- They will be expected to help specify and select systems to help monitor and enforce security across the Trust's network and corporate and clinical systems
- The post holder is responsible for budget setting for several services,

Management/Leadership

- The postholder will be called upon to delivers training in cyber security to other staff and organisations.
- They are expected to maintain, refresh and continually develop their own skill set and knowledge.

Information Resources

- The postholder is responsible for ensuring the security and integrity of information and secure access to the systems.

Research and development

- The postholder will be required to assist in information collection, collation and presentation for audit, survey, research and reporting purposes.

Freedom to Act

- The postholder is expected to work under their own initiative, but within National guidelines, local policies and standard operating procedures.
- They will be expected to interpret how policies should be implemented within the service and wider organisation using their judgement and expert knowledge to ensure the best outcome for the organisation requirements and ensuring a sustainable service

Physical effort

- There is a frequent requirement for sitting or standing in a restricted position for a substantial proportion of the working time,

Mental effort

- There is a frequent requirement for concentration where the work pattern is predictable with few competing demands for attention

Emotional Effort

- Occasional exposure to distressing or emotional circumstances.

Working conditions

- Requirement to use Visual Display Unit equipment more or less continuously on most days.

Person Specification

Criteria	Essential	Desirable	***How criteria will be assessed***
Qualifications	• Degree in a computer related subject / Level 4 Apprenticeship in IT Or • An equivalent level of knowledge and expertise acquired by experience • Willingness to study and complete additional cyber	• ITIL foundation or equivalent • CISSP (Certified Information Systems Security Professional) • Understanding of NHS standards, practices and operations	Certificates Application Interview

	courses and qualifications • Relevant post graduate cyber specific qualifications, i.e. CISSP, relevant product specific training in SIEM / AV / Vulnerability scanning etc, technical qualifications i.e. MCSE etc Or An equivalent level of knowledge and expertise acquired by experience	• Experience of non-Microsoft Operating systems such as Unix/Linux	
Experience	• Experience of customer service/support • Experience of supporting endpoint computers • Experience of supporting the Windows operating system and standard office applications • Experience of supporting mobile technologies • Experience of cyber tools such as vulnerability scanners, SIEM solutions, Anti-Virus solutions etc		Certificates Application Interview
Knowledge	• A good knowledge of computer architecture and the Windows operating system • A good knowledge of directory services, messaging, endpoint security, and patch management. • A good knowledge of network architecture and firewalls • The principles of cyber security, cyber risk and cyber threats	• Information security management frameworks, such as ISO27001 • Knowledge of Change, Release and Configuration Management • Data Protection Act 1998 and GDPR • NHS Information Security and Governance Policies • The Data Security Protection Toolkit	Certificates Application Interview

		• Cyber Essentials Plus	

Compliance statement to expected organisational standards.

To comply with all Trust Policies and Procedure, with particular regard to

- Risk Management
- Health and Safety
- Confidentiality
- Data Quality
- Freedom of Information
- Equality Diversity and Inclusion
- Promoting Dignity at Work by raising concerns about bullying and harassment
- Information and Security Management and Information Governance
- Counter Fraud and Bribery

The Trust has designated the prevention and control of healthcare associated infection (HCAI) as a core patient safety issue. As part of the duty of care to patients, all staff are expected to:
Understand duty to adhere to policies and protocols applicable to infection prevention and control.

- Comply with key clinical care policies and protocols for prevention and control of infection at all time; this includes compliance with Trust policies for hand hygiene, standards (universal) infection precautions and safe handling and disposal of sharps.
- All staff should be aware of the Trust's Infection Control policies and other key clinical policies relevant to their work and how to access them.
- All staff will be expected to attend prevention and infection control training, teaching and updates (induction and mandatory teacher) as appropriate for their area of work, and be able to provide evidence of this at appraisal.

- To perform your duties to the highest standard with particular regard to effective and efficient use of resources, maintaining quality and contributing to improvements.

- Ensure you work towards the Knowledge and Skills Framework (KSF) requirements of this post. KSF is a competency framework that describes the knowledge and skills necessary for the post in order to deliver a quality service.

- Your behaviour will demonstrate the values and vision of the Trust by showing you care for others, that you act professionally as part of a team and that you will continually seek to innovate and improve. Our vision, values and behaviours have been designed to ensure that everyone is clear about expected behaviours and desired ways of working in addition to the professional and clinical requirements of their roles.

- Ensure you adhere to and work within local and national safeguarding children legislation and policies including the Children Act 1989 & 2004 , Working Together to Safeguard Children 2013, 4LSCB guidance and the IOW Safeguarding Policy.

- Ensure you adhere to and work within the local Multiagency safeguarding vulnerable adults policies and procedures

- Ensure that you comply with the Mental Capacity Act and its Code of Practice when working with adults who may be unable to make decisions for themselves,

- Ensure that you maintain personal and professional development to meet the changing demands of the job, participate in appropriate training activities and encourage and support staff development and training.
- Respect the confidentiality of all matters that they may learn relating to their employment and other members of staff. All staff are expected to respect conform to the requirements of the Data Protection Act 1998, including the responsibility to ensure that personal data is accurate and kept up to date

- If your employment is to a post that requires you to be registered with a professional body, the continuation of your employment is conditional upon you continuing to be registered with the appropriate professional body. The Trust will require evidence of current registration.

- Proactively, meaningfully and consistently demonstrate the Trust Values in your every day practice, decision making and interactions with patients and colleagues.

- Perform any other duties that may be required from time to time.

- Contribute to the IT Departments on-call rota and if required, maintain required skills, experience and resource levels allowing for hospital digital 24/7 services.

This job description may be altered, from time to time, to meet changing needs of the service, and will be reviewed in consultation with the post holder.