Royal Devon University Healthcare NHS Foundation Trust

JOB DESCRIPTION

JOB DETAILS	
Job Title	Cyber Security Specialist
Reports to	Head of Digital Infrastructure
Band	Band 6
Department/Directorate	Digital Services (North)

JOB PURPOSE

Under the operational management of the Head of Digital Infrastructure, the role provides specialist support and analysis of the Trust's Digital security systems, network technical security requirements and security incident events; to maintain and develop the highest level of IT security, ensuring that the Trust's digital infrastructure and applications comply with best practice, along with technical, health records, cyber, and physical security standards.

The role is accountable to the Trust's Cyber Security Lead providing assurance that they are operating to industry standards, meeting cyber ethics and codes of conducts and NHS national frameworks.

This role will be key in supporting the Digital Transformation at the Trust by contributing to both the Security strategy as well as the wider Digital programmes over the coming years.

The Cyber Security Specialist role is vital in ensuring that the Trust is compliant with Local/National policy and technology elements of the Data Security & Protection Toolkit managed within Digital Services.

The role will also be responsible for managing and reporting of Cyber Security events and ensuring any actions from audits have assigned action owners and are followed up within the specified time frames.

The role will operate a robust internal assurance framework to ensure that information assets are assessed against information security controls with appropriate action plans identified.

The Cyber Security Specialist will be based at Northern Devon District Hospital (NDDH) / Devonshire House, however, will work closely with the wider RDUH Digital Service, clinical leads and broader Trust staff based at NDDH, Exeter and all Community / remote office locations.

The post holder will fulfil required Digital Cyber Security tasks, support the development of complex analytical / reporting tools, responsible for updating and implementing process and associated standard operating procedures (SOP's), lead on Trust raised cyber security risk and issues relevant to own service and work as part of an extensive team; they will need to work with staff across all areas and levels within the Trust to ensure that the requirements relating to cyber security agenda are carried out.

To meet the needs of the service, the post holder may be required to work in other administrative areas as appropriate and as directed by the line manager and may, on occasion, be required to both manage and supervise external staff e.g. temps, contractors, external IT vendors any agency staff.

Maintains constructive relationships with a broad range of internal and external stakeholders across the NHS and wider working partnerships.

KEY RESULT AREAS/PRINCIPAL DUTIES AND RESPONSIBILITIES

- Provides specialist advice, leads on, and performs day-to-day operation of, the Trust's defences against cyber threats and against breaches of IT security protections;

- Provides guidance on the selection, design, justification, implementation and operation of digital security strategies, technologies, processes, procedures and standards
- Supports the implementation of controls to maintain the safety, confidentiality, integrity, availability and security of the Trust's digital infrastructure and systems along with the protection of Trust and patient data, both stored and processed by infrastructure or applications managed by, or under the control of, the Trust.
- Assist Digital Service leads, Technology Specialists and Information Asset Owners to ensure best practices are developed when implementing / changing Trust's digital services and that all system security issues and risks are managed.
- Provides specialist assistance to Digital Services on technical security issues including hands on technical configuration and day-to-day operation of devices and software. The post holder will also be required to keep up-to-date with the latest cyber and physical security techniques and technologies, to enable the Trust to maintain information security to the highest standards.
- Provides specialist analysis of developments to the Trust's Digital Services, to ensure they are aligned with Trust, regional, and national digital strategies and comply with industry technical security requirements and standards.
- The post holder is required to be the designated specialist on cyber security information and event management tools for Digital Services and provide an expert, specialist advice service, in accordance with national and local cyber security policies and best practice; including development of others in this capability.
- The post holder will be expected to assist Service Managers / IAO's in identifying areas in which the Trust is inadequately covered by manual and automated procedures and, in consultation with the network, data protection, information governance, technical leads and line management, develop new procedures to cover these areas, in line with policy and process. Also, the post holder will be required to support Digital Services management in presenting these procedures to the relevant non-technical stakeholders.

Digital Services Security Operations:

- To operate as the Digital Security Specialist in matters relating to Information/Cyber Security event monitoring. Provide advice and guidance regarding the implementation of security standards and procedural controls to mitigate malicious or unauthorised actions.
- Undertake daily operational maintenance and monitoring of security systems as directed by the Digital Services senior stakeholders, to apply security checks and provide advice, guidance and leadership on any subsequent remediation; providing analysis, tracking and response to multiple types of security exception cases – attacks, vulnerabilities and breaches.
- Provide analysis and responses to requests for change; including policy exceptions, removable media exceptions, workstation local admin access, workstation software exceptions and application penetration test exceptions.
- Ensure that standard security operating procedures are documented, communicated and working effectively.
- Ensure daily security operations are undertaken which include but not limited to:
    - End-point security protection, maintenance, monitoring and alerts
    - Monitoring of network access control and other access control systems
    - Regular vulnerability scanning and remediation
    - Patch management
    - Monitoring and reviewing Proxy logs, firewall logs, reports and alerts. This includes web and mail filtering, intrusion detection and prevention systems and malware protection.

- Provide assistance to Service Managers / IAO's with demonstrating the feasibility of changes to the digital environment – be they hardware, software or other system components, so that they comply with the information security requirements.
- To provide assistance to Service Managers / IAO's with addressing digital security issues as and when they arise; both long term remediation and short duration incidents.
- To provide specialist assistance with analysis of the effectiveness of existing digital security solutions, to help balance security risks and costs.

Cyber Security Incident Response:

- Deliver the necessary technical incident response and resolution activities following a suspected or actual security incident or breach. This includes, acting on all cyber security alerts received from external agencies, e.g. NHS Digital's Care CERT, are appropriately risk assessed and appropriate measures put in place to mitigate any risks that are identified.
- Providing specialist technical input to cyber security incident escalation, response and communication.
- Collaboration with 3rd parties relating to any cyber incident response.

Business Continuity and Disaster Recovery:

- Assist and contribute technical guidance to the development of Disaster Recovery Plans and the Business Continuity Management arrangements for key information assets. Ensure cyber security confidentiality, integrity and availability is maintained in the event of a disaster – and to periodically test this to ensure the documentation, processes and procedures remain current.

Projects and Governance:

- To be the security operations subject matter expert for security related projects.

Cyber Security Risk Management:

- Ensuring any cyber security risks identified by operational security procedures are recorded on the Trust's risk register
- Participate and actively input into the Digital Services risk and change management.
- Regularly review relevant Cyber Security risks, ensure risk mitigation plans are in place and regular progress reports escalated to senior Digital stakeholders.

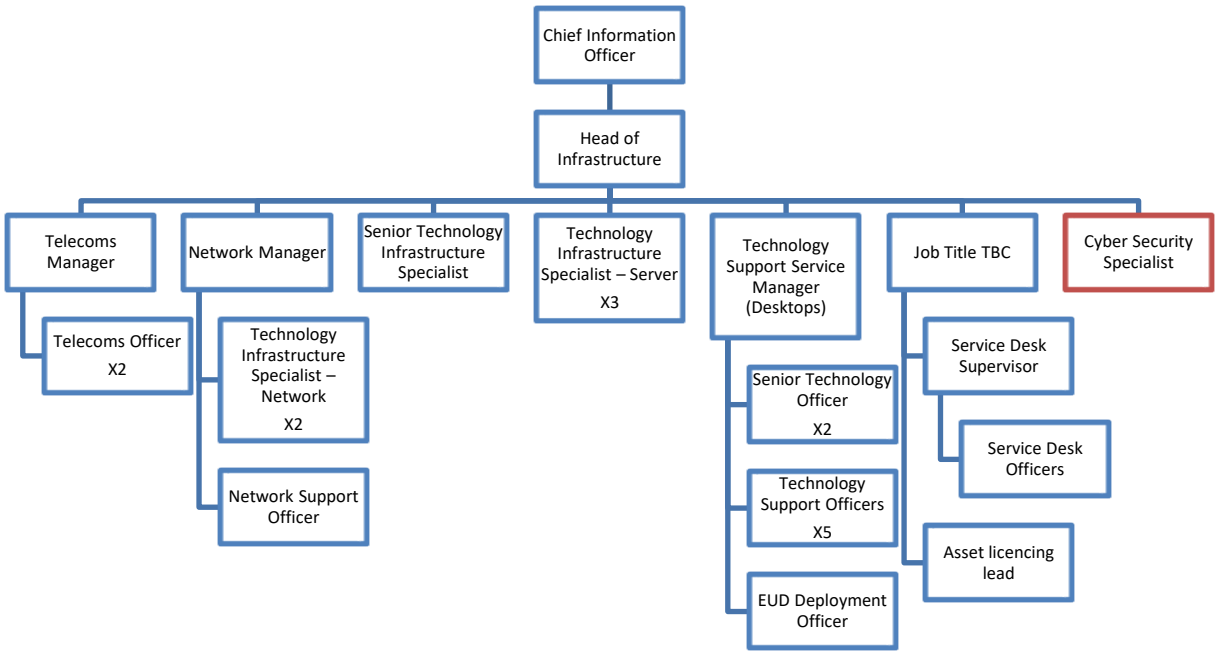
KEY WORKING RELATIONSHIPS

The post holder is required to deal effectively with staff of all levels throughout the Trust, the wider Healthcare community, external organisations and the public. This will include verbal, written and electronic media.

Of particular importance are working relationships with:

Internal to the Trust	External to the Trust
• Digital Services Staff (including Senior Management Team) • Trust Staff (all levels)	• Suppliers and vendors • Third-party Support Services • Other NHS Trusts within the South West Domain • Devon County Council • Other NHS Organisations. • Local Government

ORGANISATIONAL CHART



FREEDOM TO ACT

- The post holder will work to achieve agreed objectives and have freedom to do this in their own way, working within broad professional policies.
- They will advise without reference to their manager and act as a lead specialist Cyber Security.

COMMUNICATION/RELATIONSHIP SKILLS

- The post holder must be able to develop and maintain communication with people on complex matters, issues and ideas and/or in complex situations; be able to absorb complex information quickly, be articulate at communicating complex technical matters to senior non-technical staff clearly and in a manner whereby they are able to fully understand the issues, utilising both written and verbal communication skills. They will also be required to advise senior digital stakeholders on cyber security and influence the decision-making process.
- They must be able to communicate with users at all levels within the Trust. They must be able to explain very complex IT security issues and theories in a non-technical manner to a variety of internal and external audiences.
- To communicate with Third Party suppliers and other members of staff effectively where required to ensure completion of fault rectification.

ANALYTICAL/JUDGEMENTAL SKILLS

- Plan, develop and evaluate methods and processes for gathering, analysing, interpreting and presenting data and information. The post holder will need to provide, when required, detailed information and data regarding hardware and software in relations to security. Information will need to be articulated at times to both technical and non-technical staff at all levels.
- The role requires generation, collection and analysis of data used to provide detailed comprehensive security reporting. Reporting will be used to provide the information to the senior digital stakeholders and used to analyse growth trends and identify future requirements.
- The post holder will need to be able to provide information and data in order to present information for departmental monthly reports.

PLANNING/ORGANISATIONAL SKILLS

- The post holder will be required to undertake tasks and activities which may require adjustment due to variable workload. They will initiate plans and modify Digital work programmes.

PATIENT/CLIENT CARE

- The post holder is required to put the patient, as the first priority, at the centre of all activities although the post holder will not have contact with patients in the course of their normal duties.

POLICY/SERVICE DEVELOPMENT

- Assisting with Security Gap Analysis against Industry standards and the production of a Digital Security Improvement Programme (as part of the Strategy) that meets the digital security baselines contained within NHS Digital Data Security and Protection requirements and any new standards that are introduced.
- Provide specialist technical contribution into drafting and/or maintaining of the Trust's formal Digital Security related policies.
- Provide specialist technical contributions to the development of the Trust's security related technical policies and controls for the secure operation of digital Infrastructure and applications. This includes assisting with:
    - The assurance that adequate access control mechanisms are in place and can be audited on a regular basis.
    - Development and maintenance of the technical implementation of policies, standards and controls for digital security across the Trust.
    - Cyber security audits and using the results to improve the effectiveness of the security controls.
    - Providing regular cyber security assurance and exception reports to Digital leadership.
    - Ensuring poor security practices are reported to the appropriate governance groups.
    - Checking existing processes and procedures in place are being adhered to and that improvement plans exist to correct any non-conformances.
    - Work with accredited third parties to undertake regular vulnerability assessments, penetration tests and audits. Undertake any subsequent work plans to mitigate any risks highlighted.
    - Ensuring that appropriate security controls and safeguards are in place for each asset detailed on the Trust's Information Asset Register.
    - Establishing a standard set of functional and non-functional security requirements for application software; web, mobile and cloud applications.

FINANCIAL/PHYSICAL RESOURCES

- Provide technical security advice on the procurement, implementation, operation and maintenance of digital solutions.
- Work with Service Managers and IAO's to ensure that all 3rd party digital support contracts and supplier meet Trust cyber security standards and to report the status of these on a regular basis.

HUMAN RESOURCES

- Undertake the knowledge sharing and briefing sessions for staff on Cyber Security and ensure the Cyber Security awareness is effective and functional.
- Keep abreast of current developments within the Cyber Security and related industries.
- Work with the Trust's Communications Team to formulate communication across the Trust to raise awareness and alertness to any cyber threats and best practices.

INFORMATION RESOURCES

- The post holder will regularly be required to create, develop and present reports and documents to stakeholders. They will be responsible for maintaining information systems, and adapt these systems to meet the specifications of others.

RESEARCH AND DEVELOPMENT

- The post holder will be required to test and adapt Digital systems.

PHYSICAL SKILLS

- Advanced keyboard use – able to use multikey combinations.
- Inputting and manipulating data and information into computer systems.
- Uses fine tools with accuracy when working on IM&T systems

PHYSICAL EFFORT

- Required to spend extended periods of time in front of a VDU / PC.

MENTAL EFFORT

- To undertake on a regular basis complex analysis, report/policy writing and incident investigation, requiring long periods of concentration with some interruption.

EMOTIONAL EFFORT

- Cyber Security is a high-profile subject and there may be periods of time when this role is exposed to sensitive situations.
- The post holder will undertake other duties as may be required to achieve the Trust's objectives, commensurate with the grading of the post.

WORKING CONDITIONS

- Long periods of working day in front of VDU equipment up to 4-5 hours, however with frequent breaks and interruptions.
- Busy Office environment.
- Working with and around IT equipment.
- Working with electrical equipment.
- IT Comm's and Server rooms produce levels of heat and noise relative to the environment expected to work up to 1-2 hours a week in these environments.
- Visiting and working within varying acute and community locations weekly.

OTHER RESPONSIBILITIES

Take part in regular performance appraisal.

Undertake any training required in order to maintain competency including mandatory training, e.g. Manual Handling

Contribute to and work within a safe working environment

You are expected to comply with Trust Infection Control Policies and conduct him/herself at all times in such a manner as to minimise the risk of healthcare associated infection

As an employee of the Trust, it is a contractual duty that you abide by any relevant code of professional conduct and/or practice applicable to you. A breach of this requirement may result in action being taken against you (in accordance with the Trust's disciplinary policy) up to and including dismissal.

You must also take responsibility for your workplace health and wellbeing:

- When required, gain support from Occupational Health, Human Resources or other sources.

- Familiarise yourself with the health and wellbeing support available from policies and/or Occupational Health.
- Follow the Trust's health and wellbeing vision of healthy body, healthy mind, healthy you.
- Undertake a Display Screen Equipment assessment (DES) if appropriate to role.

GENERAL

This is a description of the job as it is now. We periodically examine employees' job descriptions and update them to ensure that they reflect the job as it is then being performed, or to incorporate any changes being proposed. This procedure is conducted by the manager in consultation with the jobholder. You will, therefore, be expected to participate fully in such discussions. We aim to reach agreement on reasonable changes, but if agreement is not possible, we reserve the right to insist on changes to your job description after consultation with you.

Everyone within the Trust has a responsibility for, and is committed to, safeguarding and promoting the welfare of vulnerable adults, children and young people and for ensuring that they are protected from harm, ensuring that the Trusts Child Protection and Safeguarding Adult policies and procedures are promoted and adhered to by all members of staff.

PERSON SPECIFICATION

Job Title	Cyber Security Specialist

Requirements	Essential	Desirable
QUALIFICATION/ SPECIAL TRAINING		
Educated to Degree and Post Graduate standard or equivalent in an IT related subject or with equivalent experience learning in a digital field.	E	
Proven experience within NHS support Cyber Security agenda		D
Specialist knowledge / Qualifications / relevant proven experience: Cyber Security	E	
Formal accredited Technology qualification (Desktop, Service Desk, Mobile, Data, Security, Project, COBIT)		D
Certified Information Systems Security Professional qualification or equivalent experience.		D
KNOWLEDGE/SKILLS		
Excellent written and verbal communication skills.	E	
Ability to provide, receive and use complex and commercially sensitive information.	E	
High level of analytical thinking and problem-solving skills.	E	
Relevant Information security standards and associated controls.	E	
Able to present complex information clearly / accurately.	E	
Relevant knowledge of cyber threats and vulnerabilities and sources of Information.	E	
Cryptographic controls		D
Cloud Technologies		D
Patch Management and change solutions		D
EXPERIENCE		
Admin and config of Security Incident monitoring Tools	E	
NHS or equivalent public sector organisation experience		D
Incident Response Management	E	
Vulnerability Assessment techniques	E	
Excellent understanding of digital services technology models.	E	
Risk management techniques	E	
PERSONAL ATTRIBUTES		
Able to work as a team member	E	
Well-developed reporting skills		D

Flexible approach to work Able to organise working environments in a way that is conducive to working practices. Ability to use own judgement and decision making at a Technology specialist level	E E E	
OTHER REQUIREMENTS The post holder must demonstrate a positive commitment to uphold diversity and equality policies approved by the Trust. Ability to travel to other locations as required.	E E	

Complete the table below as appropriate

WORKING CONDITIONS/HAZARDS		FREQUENCY (Rare/ Occasional/ Moderate/ Frequent) R	O	M	F
Hazards/ Risks requiring Immunisation Screening					
Laboratory specimens	N				
Contact with patients	N				
Exposure Prone Procedures	N				
Blood/body fluids	N				
Laboratory specimens	N				
Hazard/Risks requiring Respiratory Health Surveillance					
Solvents (e.g. toluene, xylene, white spirit, acetone, formaldehyde and ethyl acetate)	N				
Respiratory sensitisers (e.g isocyanates)	N				
Chlorine based cleaning solutions (e.g. Chlorclean, Actichlor, Tristel)	N				
Animals	N				
Cytotoxic drugs	N				
Risks requiring Other Health Surveillance					
Radiation (>6mSv)	N				
Laser (Class 3R, 3B, 4)	N				
Dusty environment (>4mg/m3)	Y				
Noise (over 80dBA)	Y	x			
Hand held vibration tools (=>2.5 m/s2)	N				
Other General Hazards/ Risks					
VDU use (> 1 hour daily)	Y				x
Heavy manual handling (>10kg)	Y	x			
Driving	N				
Food handling	N				
Night working	N				
Electrical work	N				
Physical Effort	Y		x		
Mental Effort	Y				x
Emotional Effort	Y		x		
Working in isolation	Y		X		
Challenging behaviour	Y	x			