

JOB DESCRIPTION

JOB DETAILS:

Job Title:	IT Cyber Security Analyst
Band:	5
Service Group:	Corporate Services Group
Department:	Digital Services
Base:	Taunton (Various)/Yeovil (Various)
Responsible for:	
Responsible to:	IT Cyber Security Manager

Job Purpose

The Cyber Security Analyst role is to assist in the planning, organisation and execution of Cyber Security tasks as assigned by the Cyber Security Manager ensuring the security and resilient operation of Trust and (but not limited to) its current customers' IT infrastructures. This includes monitoring, maintaining, supporting, and optimising key Cyber security areas such as Network and Server infrastructure, Networks and Data communications. The Cyber Security Analyst will also schedule and direct activities to resolve cyber security incidents and requests in a timely and accurate fashion.

There is an expectation of out-of-hours (anti-social hours) support to deal with system upgrades/failures as required by the line manager.

There will be a requirement to be involved with the out of hours' service rota as required. This involves having the appropriate skills to ensure emergency call outs are handled as quickly as possible and escalating faults to other on-call teams and the On-call Manager where necessary.

Principle Duties and Responsibilities :

- Provide technical support and advice on cyber security issues and incidents.
- Monitor and maintain cyber security system performance.
- Respond to Cyber security alerts received by the Trust in line with internal processes and timescales.
- Respond and record in line with internal process to NHS digital Cyber alerts/CareCERT Notifications.
- Assist in the monitoring and testing of the security of IT Infrastructure.
- Assist in maintenance of the Cyber Security infrastructures and to ensure integration with national and local IT services.

Date of Job Description: July 2025



Duties and Responsibilities

Communication and Key Working Relationships

The postholder will be required to provide Cyber Security and technical support for a wide range of hardware and software. This will involve communicating complex technical and non-technical information, to internal / external colleagues, and suppliers. This will also include:

- Effectively communicate in a variety of ways, including verbal, electronic and written communications. This may include presenting reports and attending meetings.
- Communicate sensitive/complex information to internal and external colleagues and other key stakeholders.
- Respond and record in line with internal process to NHS digital Cyber alerts/CareCERT Notifications.
- Escalating unsolved problems to IT Cyber Security Manager.
- Keep users informed regarding status of outstanding issues.
- Communicate progress on project plans to relevant parties ensuring they are kept informed of progress
- Ensure lessons learned are documented, shared with colleagues and acted upon, to support continued service improvement.
- Produce and review technical documentation

The postholder will be required to be in regular contact with:

- 1st, 2nd and 3rd Line Support and other Technical Staff.
- Senior Managers, Directorate and Department Managers
- Users/clinical staff
- Suppliers/3rd party users
- External colleagues from local, regional and national health and social care providers/commissioners.

Planning and Organisation

- The postholder will be required to manage the planning and organisation of own workload, including prioritisation. This will happen on a daily basis due to the nature of work and interruptions required to deal with unplanned events.
- Consider the impact of digital system change on patients/clients, carers, relatives and/or colleagues.
- Consider the impact of change on clinical safety and patient/client services.
- Work mainly on own initiative and manage the planning/organization of own workload.

Work with project managers, customers, suppliers and other Digital teams to support the implementation of cyber security and technical projects or development in IT from conception to implementation and handover:

- Provide cyber security and technical advice, guidance and support to Digital



teams and staff across the organization.

- Responsible for processing service requests in a timely fashion and ensuring appropriate response times are met
- Investigate technical requirements and solutions. This may involve meetings with suppliers, reading technical documents and carrying out practical testing
- Undertake research into technical solutions ensuring they comply with NHS standards and regulations
- Demonstrate new technology, systems or processes
- Assist other Digital teams in projects at an appropriate level for post

Analytics

N/A

Responsibility for Patient / Client Care, Treatment & Therapy

- Contribute to the setting of Key Performance Indicators (KPIs) and managing performance to achieve these.

Policy, Service, Research & Development Responsibility

Postholder will be required to:

- Be a contributor to the Cyber Security Strategy and other relevant technological developments.
- Contribute to the development and implementation of Cyber Security policies and procedures within the Trust.
- Ensure policies, procedures and processes are documented, reviewed and updated.
- Contribute to the implementation of policies and procedures within the service area, ensuring compliance with relevant standards (including clinical safety and data security and protection).
- Handle confidential information in accordance with current policies and procedures.
- Role will require postholder to make recommendations on new technologies to be used to ensure the service provided to customers is efficient and cost effective.
- Keep abreast of legislation and NHS guidance relating to digital services and especially Cyber Security.

Responsibility for Finance, Equipment & Other Resources

The postholder will:

- Have shared responsibilities for the security of IT premises, eg computer rooms, comms and IT Buildings and office accommodation.
- Take responsible for the safety and security of any device allocated and for the working environment; the use of all digital systems, including any storage and movement of data, should be done in accordance with the organisations data security and protection policy.



- Ensure the safe keeping of IT equipment under postholder's care, including transit to other sites.

Responsibility for Supervision, Leadership & Management

None

Information Resources & Administrative Duties

The postholder will be responsible for dealing with requests from 1st, 2nd and 3rd line support. This includes updating status and notes for support tickets along with detailed notes on progress and resolution information.

Main duties undertaken by the postholder will include:

- Provide technical support and advice on cyber security issues and incidents.
- Monitor and maintain cyber security system performance.
- Assist in the monitoring and testing of the security of IT Infrastructure.
- Assist in maintenance of the Cyber Security infrastructures and to ensure integration with national and local IT services.
- Contribute and assist in the Development of IT Security testing frameworks.
- Assist in the management, monitoring and development of patch management processes
- Assist with the annual cyber/security accreditation process.
- Contribute to research, planning and deployment and monitoring of cyber security measures for infrastructure and systems.
- Test server, application and database security, providing statistics and reporting when required.
- Practice IT hardware & software asset management, including maintenance of component inventory and related documentation.
- Assist in the establishment, management and monitoring of supplier/customer performance contracts and service level agreements.
- Contribute to and assist with PIA and IT procurement requests.
- Contribute to the design, implementation and testing of Trust IT disaster recovery and business continuity systems.
- Assist IT Cyber Security Manager in the regular maintenance and testing of the IT DR/BC testing regime.

Any Other Specific Tasks Required

- The Post holder will supervise IT contractors when working on customer & IT Services sites to ensure correct procedures are followed
- The post is required to work in a technical environment without supervision and may only have contact with a line manager once a week



Review of this Job Description

This job description is intended as an outline indicator of general areas of activity and will be amended in the light of changing service needs. This job description is to be reviewed in conjunction with the post holder on an annual basis.

General Information

At all times promote and maintain the safety of children by working according to the Trust's Child Protection Policy and supporting guidance. Being pro-active and responsive to child protection concerns by early reporting, recording and referral of issues according to Trust arrangements. Attending child protection training that is appropriate to your role.

Confidentiality

The post holder will maintain appropriate confidentiality of information relating to commercially sensitive matters in regard to Trust business, and also to personal information relating to members of staff and patients. The post holder will be expected to comply with all aspects of the General Data Protection Act (2018), the Staff Code of Confidentiality and the IT Security and Acceptable Use Policy.

Equality & Diversity

Somerset NHS Foundation Trust is committed to achieving equality of opportunity for all staff and for those who access services. You must work in accordance with equal opportunity policies/procedures and promote the equality and diversity agenda of the Trust.

Safeguarding

All employees have a duty for safeguarding and promoting the welfare of children and vulnerable adults. Staff must be aware of the Trust's procedure for raising concerns about the welfare of anyone with whom they have contact.

Risk Management / Health and Safety

Employees must be aware of the responsibilities placed on them under the Health & Safety at Work Act 1974, ensure that agreed safety procedures are carried out and maintain a safe environment for employees, patients and visitors.

Smoking

The Trust operates a 'non-smoking' policy. Employees are not permitted to smoke anywhere within the premises of the Trust or when outside on official business.



Records Management

The post holder has responsibility for the timely and accurate creation, maintenance and storage of records in accordance with Trust policy, including email documents and with regard to the General Data Protection Act, The Freedom of Information Act and any other relevant statutory requirements.

Clinical Governance

The post holder will be expected to participate in clinical governance activities to assist the Trust to provide high quality services.

Prevention and Control of Healthcare Associated Infection

The post holder is expected to comply with Trust Infection Control Policies and conduct themselves at all times in such a manner as to minimise the risk of healthcare associated infection.

Policies & Procedures

Trust employees are expected to follow Trust policies, procedures and guidance as well as professional standards and guidelines. Copies of Trust policies can be accessed via the staff intranet or external website or via your manager.

Sustainability Clause

Somerset NHS Foundation Trust is committed to creating a sustainable business. Staff employed by the Trust, are required to think about their actions in the course of their work and make positive steps to reducing, reusing and recycling wherever and whenever possible.



Person Specification

This is a specification of the Qualifications, Skills, Experience, Knowledge, Personal Attributes and Other Requirements which are required to effectively carry out the duties and responsibilities of the post (as outlined in the Job Description).

Requirement	Essential / Desirable	How Assessed
<u>BEHAVIOURS ALIGNED WITH TRUST VALUES</u>		
<ul style="list-style-type: none"> Outstanding care 	E	AF/I
<ul style="list-style-type: none"> Listening and leading 	E	AF/I
<ul style="list-style-type: none"> Working together 	E	AF/I
<u>QUALIFICATIONS & TRAINING</u>		
<ul style="list-style-type: none"> Good general level of education with a minimum of GCSE Maths and English 4 or above. 	Essential	AF
<ul style="list-style-type: none"> Degree in a relevant field is required or demonstrate equivalent knowledge and skills gained through any combination of alternative study and/or previous employment 	Essential	AF
<ul style="list-style-type: none"> Cyber Security certification (CISSP, CEH, SCCP) 	Desirable	AF
<ul style="list-style-type: none"> Cyber Security training (Comptia security+) 	Desirable	AF
<ul style="list-style-type: none"> IT certification (Microsoft certified etc) 	Desirable	AF
<ul style="list-style-type: none"> ITIL Qualification 	Desirable	AF
<u>KNOWLEDGE</u>		
<ul style="list-style-type: none"> Good knowledge in the field of cyber security, securing and monitoring networks, systems and devices. 	Essential	AF/I
<ul style="list-style-type: none"> Good knowledge and experience of data networking technologies & protocols 	Essential	AF/I
<ul style="list-style-type: none"> Good technical knowledge of Operating systems (Windows, Linux etc) 	Essential	AF/I
<ul style="list-style-type: none"> Knowledge Active Directory/Azure/Entra Management 	Essential	AF/I
<ul style="list-style-type: none"> Knowledge of NHS/Health environments and National IT Programmes 	Desirable	AF/I
<ul style="list-style-type: none"> Understanding of NHS IT Policies and 	Desirable	AF/I



Strategies		
<p><u>EXPERIENCE</u></p> <ul style="list-style-type: none"> Working with 3rd party suppliers ensuring a high-quality service is delivered. Working with NHS professionals to implement information and operational systems Experience of managing priorities and participating in large projects Demonstrable evidence of working in a technical IT Environment Experience of working in an ITIL based environment with an emphasis on project management, change control, incident management, customer service and service delivery. IT Security experience within the NHS, public sector or major private sector organisation 	<p>Essential</p> <p>Essential</p> <p>Essential</p> <p>Essential</p> <p>Desirable</p> <p>Desirable</p>	<p>AF/I</p> <p>AF/I</p> <p>AF/I</p> <p>AF/I</p> <p>AF/I</p> <p>AF/I</p>
<p><u>SKILLS & ABILITIES</u></p> <ul style="list-style-type: none"> Previous experience of working in a large public sector or corporate IT department Developing technical protocols and documentation Strong analytical and problem-solving skills 	<p>Essential</p> <p>Essential</p> <p>Essential</p>	<p>I</p> <p>I</p> <p>I</p>
<p><u>COMMUNICATION SKILLS</u></p> <ul style="list-style-type: none"> Evidence of a good standard of Literacy / English language skills Ability to convey complex information to both technical and non-technical staff Able to work in a team with good interpersonal skills including tact and discretion. Ability to communicate clearly with Digital Services colleagues, senior managers, clinicians and external contractors. High standard of written and verbal communication 	<p>Essential</p> <p>Essential</p> <p>Essential</p> <p>Essential</p> <p>Essential</p>	<p>I</p> <p>I</p> <p>I</p> <p>I</p> <p>I</p>
<p><u>PLANNING & ORGANISING SKILLS</u></p>	<p>Essential</p>	<p>I</p>



<ul style="list-style-type: none"> • Excellent analytical and problem-solving skills with ability to analyse, interpret and resolve issues relating to complex Cyber security and IT issues • Accurately follow documented procedures • Ability to plan a range of ongoing service activities some with interdependencies including small scale project management to meet service delivery requirements • Ability to priorities task according to business and service impact. • Ability to meet objectives and work under pressure 	<p>Essential Essential</p> <p>Essential</p> <p>Essential</p>	<p>I I</p> <p>I</p> <p>I</p>
<p><u>PHYSICAL SKILLS</u></p>		
<p><u>OTHER</u></p> <ul style="list-style-type: none"> • Willingness to use technology to improve standards of care and support to our patients • Enthusiastic • Willing to learn • Self-motivated • Pro-active • Able to remain calm under pressure • Organised • Attention to detail • Effective teamwork • Able to remain calm under pressure • Current full UK driving licence (Minimum category B / B1) • Access to a car or other private transport • Ability to deal with and manage conflict 		
<p>SUPPORTING BEHAVIOURS</p> <p>To carry out this role successfully the post holder needs to be fully aware of and adhere to Trust values.</p> <ul style="list-style-type: none"> • Kindness • Respect • Teamwork 		



SUPPLEMENTARY INFORMATION

Physical Effort	Yes	No	If yes – Specify details here (Incl. duration and frequency)
Working in uncomfortable / unpleasant physical conditions	Yes		Occasional requirement i.e. when tracing cables install server and network equipment
Working in physically cramped conditions	Yes		Occasional requirement i.e. when tracing cables install server and network equipment
Lifting weights, equipment or patients with mechanical aids		No	
Lifting or weights / equipment without mechanical aids	Yes		Occasional requirement to move IT equipment including UPS's and servers
Moving patients without mechanical aids		No	
Making repetitive movements		No	
Climbing or crawling	Yes		Occasional requirement i.e. when tracing cables
Manipulating objects		No	
Manual digging		No	
Running		No	
Standing / sitting with limited scope for movements for long periods of time	Yes		When desk based carrying our admin duties
Kneeling, crouching, twisting, bending or stretching	Yes		Occasional requirement i.e. when tracing cables install server and network equipment
Standing / walking for substantial periods of time	Yes		Requirement to visit multiple parts of the hospital
Heavy duty cleaning		No	
Pushing / pulling trolleys or similar	Yes		Occasional requirement when installing IT equipment
Working at heights		No	
Restraint ie: jobs requiring training / certification in physical interventions		No	
Mental Effort	Yes	No	If yes – Specify details here (Incl. duration and frequency)
Interruptions and the requirement to change from one task to another (give examples)	Yes		Regular requirement to change tasks based on urgency of incoming work
Carry out formal student / trainee assessments		No	
Carry out clinical / social care interventions		No	
Analyse statistics		No	
Operate equipment / machinery		No	
Give evidence in a court / tribunal / formal hearings		No	
Attend meetings (describe role)	Yes		Team/Departmental meetings, meetings with suppliers and 3 rd



			parties
Carry out screening tests / microscope work		No	
Prepare detailed reports	Yes		Complete reports as required
Check documents	Yes		Check update support documentation as required
Drive a vehicle	Yes		Requirement to visit multiple sites
Carry out calculations		No	
Carry out clinical diagnosis		No	
Carry out non-clinical fault finding		No	
Emotional Effort	Yes	No	If yes – Specify details here (Incl. duration and frequency)
Processing (eg: typing / transmitting) news of highly distressing events		No	
Giving unwelcome news to patients / clients / carers / staff		No	
Caring for the terminally ill		No	
Dealing with difficult situations / circumstances		No	
Designated to provide emotional support to front line staff		No	
Communicating life changing events		No	
Dealing with people with challenging behaviour		No	
Arriving at the scene of a serious incident		No	
Working conditions – does this post involve working in any of the following:	Yes	No	If yes – Specify details here (Incl. duration and frequency)
Inclement weather		No	
Excessive temperatures		No	
Unpleasant smells or odours		No	
Noxious fumes		No	
Excessive noise &/or vibration		No	
Use of VDU more or less continuously	Yes		When desk based carrying our admin duties
Unpleasant substances / non household waste		No	
Infectious Material / Foul linen		No	
Body fluids, faeces, vomit		No	
Dust / Dirt		No	
Humidity		No	
Contaminated equipment or work areas		No	
Driving / being driven in Normal situations	Yes		Requirement to visit multiple sites
Driving / being driven in Emergency situations		No	
Fleas or Lice		No	
Exposure to dangerous chemicals / substances in / not in containers		No	



Exposure to Aggressive Verbal behaviour		No	
Exposure to Aggressive Physical behaviour		No	

Department Core Purpose

The Knowledge and Skills Framework (KSF) outline for this post which demonstrates the skills and competencies required once in post should be considered in conjunction with this document.

Job Profile Agreement

Agreed and Signed:	(Manager)	Date:	
Agreed and Signed:	(Post Holder)	Date:	
Date Role Description is Effective From:			

