NHS
East London
NHS Foundation Trust

JOB DESCRIPTION

JOB TITLE:	Senior Digital Security Specialist
BAND:	7
DEPARTMENT:	Digital
DIRECTORATE:	Digital
REPORTING TO:	Chief Information Security Officer
ACCOUNTABLE TO:	Chief Digital Officer

JOB SUMMARY

The Senior Digital Security Specialist is a key member of the Cyber Security Team within the Digital service, and will provide specialist advice in accordance with national or local IT security policies and best practice to meet its Cyber Security obligations.

- Through proactive monitoring, identify, understand, and prioritise, cyber threats or vulnerabilities and provide appropriate remediation, mitigation, or escalation.
- Support, monitor, and manage the deployment process of software updates and security patches across the Trust.
- Represent the organisation at various internal and external forums on all security related topics
- Assist with the Cyber Security assurances of the Data Security and Protection Toolkit
- Assist with the development of the Trust's Cyber Security Strategy and will contribute to the Trust's Cyber Incident Response plan
- Work closely with partners and suppliers to ensure that Cyber Security requirements are key deliverables and are incorporated into contracts
- Gather information and prepare reports of detailed metrics that demonstrate the performance of the Trust's Cyber Security defenses and mitigations.

The Senior Digital Security Specialist will maintain consistently high standards of service and ensure that the confidentiality, integrity, and availability, of the Trust's information assets are always preserved. It is expected that the post holder will have extensive technical IT skills and experience in at least one of the following:

- Server infrastructure (including Windows or Linux operating systems, and virtualisation)
- End user devices and operating systems
- Enterprise networking and firewalling

Key Working Relationships:

- The post holder will be key member of Digital Services and will work closely with other teams across the Trust in accordance with their requirements.
- The post holder will establish a close working relationship with the Information Governance service and be their point of contact for all security related issues.

External Relationships will include:

- Regulatory bodies e.g., NHS Digital, NHSX, NCSC and NHS England.
- Other Health & Care Providers
- Professional bodies

KEY RESPONSIBILITIES

Leadership and Strategic

1. To provide expert specialist Information Security advice to the Trust consistent with National and Local Security standards and best practices.

2. Working alongside the Chief Information Security Officer, and other Senior Technical Managers to assist in evaluating, recommending, and implementing infrastructure and systems that will assist with mitigating threats and vulnerabilities, and reducing the risk of a cyber-incident significantly impacting the Trust's normal operations.

3. Assist in the development of action plans to address key risks arising from assessments and assist with the development of investment cases that will improve the Trust's Cyber Security posture.

4. To work closely with the Counter Fraud Service (CFS), Police, and other external bodies when investigating incidents.

5. To contribute to the collaborative approach to Cyber Security across the Integrated Care System (ICS).

6. To assist with incident management in the event of a Cyber Incident.

Operational

1. Through proactive monitoring, identify, understand, and prioritise, threats and vulnerabilities and provide appropriate remediation, mitigation, or escalation.

2. Assist with the development, production, review, and update of IT Security documentation on all relevant Trust policies including but not limited to, Information Security & Data Protection Policy, Email Policy and Mobile Computing and Remote Working Policy.

3. To support, monitor, and manage the deployment process of all emergency updates and security patches across the Trust.

4. To assist in the administration of alert reporting and escalation or mitigation as required.

5. To promote a positive Cyber culture, ensuring the importance of good practice and policy.

6. To work closely with the relevant teams to ensure the incident planning for major incident relating to Cyberattacks are robust, and where possible undertaking any exercise that maybe helpful for our Business Continuity Planning.

7. To assist with the Cyber Security assurances of the Data Security and Protection Toolkit (DSPT).

8. To support the adoption and conformance against standards such as ISO:27001 and Cyber Essentials Plus.

9. Contribute to any Cyber awareness training the Trust need to communicate on including urgent bulletins for wider distribution across the community.

10. Work closely with partners and suppliers to ensure that Cyber Security requirements are key deliverables and are incorporated into contracts for newly provisioned systems and on any adaptations during the lifecycle systems.

Quality and Governance

1. To comply with audit requests and other requirements relating to Cyber Security as required.
2. To assist with security assessments and penetration tests carried out on our systems and infrastructure and to contribute to any associated action plans.
3. To support the gathering and presentation of metrics that demonstrate the performance of the Trust's Cyber Security defences and mitigations.

Communication

1. Communicate highly complex information and negotiate potentially contentious issues with Trust members at all levels. Including supporting local and national projects to ensure all parties are fully briefed and consulted in implementing best practice.
2. Communicate effectively on complex subjects that may impact/delay a project delivery due to unforeseen security concerns.
3. Work with the Senior Managers to ensure effective two-way communication within the department and with internal and external partners and suppliers.
4. Contribute to effective communication within the Trust and in the wider health care community regarding the Cyber Security culture and agenda.
5. Ensure that good practice is shared and delivered at all levels of the service.

Management

1. Promote a culture where staff feel empowered and accountable for the service that they provide.
2. Provide coaching and professional insight to colleagues across the organisation to ensure best practice is understood, followed, and endorsed.

Professional

1. Maintain and develop expert knowledge of current technologies, techniques, and best practice developments within the Cyber Security industry.
2. Maintain and continue with specialised certifications within Cyber Security.
3. Be able to work independently and manage own workload to make effective use of both time and resources and to work to local and national guidelines, policies, and standards.
4. Work flexibly and undertake other duties commensurate to the grade as required.
5. Participate in a joint annual Personal Development Review with line manager.

JOB DESCRIPTION AGREEMENT
This job description is intended as a guide to the main duties of the post and is not intended to be a prescriptive document. Duties and base of work may change to meet the needs of the service or because of the introduction of new technology. This job description may be reviewed from time to time and changed, after consultation with the postholder.

Statement on Employment Policies	
In addition to the requirement of all employees to co-operate in the implementation of Employment related policies, your attention is drawn to the following individual employee responsibilities:-	
Health and Safety	Under the Health & Safety at Work Act 1974 it is the responsibility of individual employees at every level to take care of their own health and safety at work and that of others who may be affected by their acts at work, and to co-operate with management in complying with health and safety obligations, particularly by reporting promptly any defects, risks or potential hazards.
Equal Opportunities	ELFT is committed to equality of opportunity for all employees, job applicants and service users. We are committed to ensuring that no one will be discriminated against on the grounds of race, colour, creed, ethnic or national origin, disability, religion, age, sex, sexual orientation or marital status. The Trust commits itself to promote equal opportunities and value diversity and will keep under review its policies, procedures and practices to ensure that all employees, users and providers of its services are treated according to their needs. For management posts, to ensure that within their service area fair employment practice and equality of opportunity are delivered.
Dealing With Harassment/ Bullying In The Workplace	The Trust believes employees have the right to be treated with respect and to work in a harmonious and supportive working environment free from any form of harassment and / or bullying. The Trust has taken positive steps to ensure that bullying and harassment does not occur in the workplace and that procedures exist to resolve complaints as well as to provide support to staff. It is your responsibility as an employee to abide by and support these steps so all employees can work in a harmonious, friendly and supportive working environment free of any harassment or intimidation based on individual differences. Disciplinary action will be taken against any member of staff found to be transgressing the Dignity at Work Policy.
No Smoking	To refrain from smoking in any of the organisations premises not designated as a smoking area. 'East London Foundation Trust is a Smokefree Trust – this means that staff must be smokefree when on duty or otherwise in uniform, wearing a badge or identifiable as ELFT staff or undertaking trust business.'
Alcohol	To recognise that even small amounts of alcohol can impair work performance and affect ones ability to deal with patients and the public in a proper and acceptable manner. Consumption of alcohol during work hours in not permitted.
Confidentiality	As an employee of the Trust the post-holder may have access to confidential information. The postholder must safeguard at all times, the confidentiality of information relating to patients/clients and staff and under no circumstances should they disclose this information to an unauthorised person within or outside the Trust. The post-holder must ensure compliance with the requirements of the Data Protection Act 1998, Caldicott requirements and the Trust's Information and IM&T Security Policy. To safeguard at all times, the confidentiality of information relating to patients/clients and staff.
General Data Protection	To maintain the confidentiality of all personal data processed by the organisation in line with the provisions of the GDPR.

Regulation (GDPR)	As part of your employment with East London Foundation Trust, we will need to maintain your personal information in relation to work on your personal file. You have a right to request access to your personal file via the People & Culture Department.
Safeguarding	All employees must carry out their responsibilities in such a way as to minimise risk of harm to children, young people and adults and to safeguard and promote their welfare in accordance with current legislation, statutory guidance and Trust policies and procedures. Employees should undertake safeguarding training and receive safeguarding supervision appropriate to their role.
Service User and Carer Involvement	ELFT is committed to developing effective user and carer involvement at all stages in the delivery of care. All employees are required to make positive efforts to support and promote successful user and carer participation as part of their day to day work.
Personal Development	Each employee's development will be assessed using the Trust's Personal Development Review (PDR) process. You will have the opportunity to discuss your development needs with your Manager on an annual basis, with regular reviews.
Quality Improvement	The Trust encourages staff at all levels to engage in the Trust's approach to quality through quality improvement projects and quality assurance.
Professional Standards	To maintain standards as set by professional regulatory bodies as appropriate.
Conflict of Interests	You are not precluded from accepting employment outside your position with the Trust. However such other employment must not in any way hinder or conflict with the interests of your work for the Trust and must be with the knowledge of your line manager.
Risk Management	Risk Management involves the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects. Every employee must co-operate with the Trust to enable all statutory duties to be applied and work to standards set out in the Risk Management Strategy.
Personal and Professional Development/Investors in People	The Trust is accredited as an Investor in People employer and is consequently committed to developing its staff. You will have access to appropriate development opportunities from the Trust's training programme as identified within your knowledge and skills appraisal/personal development plan.
Infection Control	Infection Control is everyone's responsibility. All staff, both clinical and non-clinical, are required to adhere to the Trusts' Infection Prevention and Control Policies and make every effort to maintain high standards of infection control at all times thereby reducing the burden of all Healthcare Associated Infections including MRSA. In particular, all staff have the following key responsibilities: Staff must observe stringent hand hygiene. Alcohol rub should be used on entry to and exit from all clinical areas. Hands should be washed before and after following all patient contact. Alcohol hand rub before and after patient contact may be used instead of hand washing in some clinical situations. Staff members have a duty to attend infection control training provided for them by the Trust as set in the infection control policy. Staff members who develop an infection that may be transmissible to patients have a duty to contact Occupational Health.

PERSON SPECIFICATION

JOB TITLE:	Senior Digital Security Specialist
BAND:	7
DEPARTMENT:	Digital
DIRECTORATE:	Digital
REPORTING TO:	Chief Information Security Officer
ACCOUNTABLE TO:	Chief Digital Officer

ATTRIBUTES	CRITERIA	ESSENTIAL/ DESIRABLE	SELECTON METHOD (S/I/T)
Education/ Qualification/ Training	• Educated to Masters level or equivalent experience • Suitable technical professional qualification for a senior position e.g. CISSP / CISM or equivalent experience • Evidence of relevant continuing professional development • Relevant training in network and server technologies	• ISO27001 Lead Auditor	• S/I
Experience	• Significant experience and exposure in supporting a large, complex and diverse organisation. • Significant security experience within an ISO27001 certified organisation • Demonstrable track record in implementing security related solutions	• Experience of working across organisations and with other agencies	• S/I
Knowledge and Skills	• Demonstrable in depth understanding of current NHS standards and policies relating to security • Ability to manage multiple complex projects to a successful conclusion, using structured methodologies	• Highly developed analytical skills with the ability to manage and interpret hard	• S/I

	• Substantial knowledge of Change Management processes and techniques • Working to IT service management best practice i.e. ITIL • Ability to forge long-term working partnerships with individuals and groups from internal and external departments and organisations • Ability to write clear concise reports, letters, minutes and documents using a good standard of English • Excellent organisational, problem solving, communication and analytical skills • The ability to tackle highly complex issues and resolve them to the benefit of the service. • The ability to remain current with emerging technologies • Sensible negotiator with practical expectation of what can be achieved • Track record of performance management and delivery of projects, targets, national policy implementation, change management. • Ability to facilitate large groups ensuring objectives are achieved. • Excellent oral and written communications • The ability to work under pressure to meet	and soft data.	

	agreed service levels		
Other	• Able to prioritise work, and work well against a background of change and uncertainty • Customer focused attitude to providing ICT Services • Adaptable to situations, can handle people of all capabilities and attitudes • Commitment to team-working and respect for the skills of others • Self-motivated, proactive and innovative with a 'can do' attitude and able to work with minimal supervision • Ability to promote workforce diversity and contribute to wider equality and diversity agenda	•	• S/I

S: Shortlisting I: Interview T: Test