NHS
East London
NHS Foundation Trust

JOB DESCRIPTION

JOB TITLE:	Chief Information Security Officer
BAND:	8C
DEPARTMENT:	Digital
DIRECTORATE:	Digital
REPORTING TO:	Chief Technology Officer
ACCOUNTABLE TO:	Chief Digital Officer

JOB SUMMARY

As CISO (Chief Information Security Officer), the post holder will lead and work as part of a dynamic team in delivering an effective Information Security service supporting the East London Foundation Trust.

The post holder will be an experienced senior leader, who will lead a dynamic team in delivering an effective Information Security service.

The post holder will have experience in the provision of robust governance and assurance services across the entire IT security portfolio of activities.

The post holder will have excellent stakeholder and communication skills. They will be able to lead a team to create a network of relationships necessary in the delivery of IT security, including partners such as NHSX, NHS Digital and the ICS.

KEY RESPONSIBILITIES

The Chief Information Security Officer (CISO) leads and owns the Trust's information security strategy; drives and owns the Trust's information security posture, using a risk based approach; and takes a comprehensive approach to information security. The CISO leads IT security activities within the Trust, managing the information and technology risk to the Trust's IT facilities and information from internal and external threats; advises the Trust at a strategic level on existing and emerging threats; and owns and develops the necessary IT security policies, standards and procedures.

- Develop, implement and monitor a strategic, comprehensive enterprise information security and IT risk management programme.
- Work directly with clinical and corporate functions to facilitate risk assessment and risk management processes.
- Develop, maintain and enhance an information security management framework and all related policies and processes.
- Understand and interact with related disciplines to ensure the consistent application of policies and standards across all technology projects, systems and services.
- Define and maintain the structure of the Information Security team, including any changes in staffing.
- Provide leadership to the Information Security team and virtual teams within and external to Digital Services.
- Create and maintain a strong team ethos and morale, both with direct teams and as part of the wider Digital services function.
- Ensure strong and positive day to day working relationships between the security team and all key stakeholders, in particular other parts of the Digital function.
- Represent the Trust externally as the authoritative voice in the area of information and cyber security and governance.

- Partner with business stakeholders across the Trust to raise awareness of risk management concerns.
- Assist with overall technology planning, providing a current knowledge and future vision of technology and systems.
- To lead on the Internal Audit controls for IT Security
- Manage and develop an awareness portfolio which will address the requirements of a Information Security Management System.
- Lead on the development and delivery of an effective monitoring system to measure compliance with professional and regulatory standards.
- To be responsible for providing advice and support on the investigation of all adverse events, ensure the independent review of incidents, to support the investigation, identifying the root cause and ensure that appropriate Corrective and Preventative Actions are developed, actioned and monitored.
- To collaborate with all departments within the Trust and ICS where necessary to establish a process for identification and dissemination of high quality information to facilitate effective Cyber Security management and improvement.

JOB DESCRIPTION AGREEMENT

The role of Digital Services is to ensure that the East London Foundation Trust community of clinicians and staff and its service users have access to responsive, resilient, secure and accessible systems and support. Our technologies enable our clinicians, staff, service users, visitors and partners to confidently and creatively use digital services, technology and data for in the support of providing high quality Service User care.

As a central function across Digital Services, Information Security is responsible for defining, promoting and embedding the policies, standards and processes which make us secure by design and protect our information.

The culture of Digital Services is one of innovation, collaboration, excellence and inclusivity, and we apply the principles of customer focus and continuous improvement to everything we do. We want to attract outstanding, inspirational, and talented people, support them to succeed, and celebrate their success.

Our Information Security team is a key part of Digital Services, responsible for maintaining our security tools and services, investigating and dealing with issues as they arise and supporting information security across the wider Trust.

Communication and Relationship Skills

- Develop close working relationships with all departments within NHSD and other health bodies to enable the trust’s digital service to deliver Cyber Security improvement objectives.
- Develop effective working relationships with key organisations including the NCSC, NHSD, NHSX, and other cyber security focused bodies and organisations.
- Ensure the trust share learning from professional practice and quality activities both within and outside the organisation.
- Provide leadership and direction in situations where highly complex concepts need to be conveyed and implemented across the organisation.
- Provide and receive highly complex and potentially highly sensitive information in relation to adverse events where there may be significant barriers in accepting and delivering the management of change.
- Use influencing skills to ensure collaborative working to engender a level of quality improvement across the organisation

Analytical and Judgement Skills

- Exercise judgement involving highly complex facts and figures and situations which require the analysis, interpretation and comparison of a range of options including the analysis of incidents and events.

- Analyse and assess conflicting information where opinions may differ and use critical thinking to deliver the appropriate outcomes.
- Assimilate complex data, compare facts and analyse situations from a range of sources, develop options and assess risk and opportunities for Cyber Security improvement.
- Develop, manage and facilitate appropriate corrective and preventative actions.
- Exercise specialist knowledge relating to Cyber Security processes.
- Create reports that will allow evaluation of Cyber Security improvement options.
- Interpret complex data to feed into education and training and support service improvement, redesign and delivery.
- To analyse complex data relating to Cyber Security improvement, to benchmark within and outside the trust and determine a range of options for addressing the areas identified for improvement.
- Monitor trends, observations and errors throughout the trust.

Planning and Organisational Skills

- Ensure effective review of practice and Cyber Security activities to identify their contribution for delivery against improvement programmes.
- Ensure appropriate Corrective and Preventative Actions are implemented in line with best practice guidance.
- Develop a process for Cyber Security improvement across the organisation
- Ensure effective review of accreditation requirements and their contribution in delivery to improvement programmes.
- Plan and prioritise own work ensuring effective support to all areas and delivery of key Cyber Security improvement objectives.
- Agree and manage timescales with stakeholders in Cyber Security improvement projects.
- Support the production of Cyber Security improvement documentation and post implementation evaluation.

Responsibility for Service User / Client Care

- To ensure that the needs of clinicians and Service Users are taken fully into account when planning Cyber Security improvement strategies and plans.
- Manage systems for ensuring that staff, where required, within the organisation are trained and updated in Cyber Security skills specific to their area of practice this will include Change management, Root Cause Analysis and error management and develop joint responsibility with line managers

Responsibility for Policy / Service Development Implementation

- Responsible for ensuring that effective Cyber Security improvement is implemented across the organisation.
- To lead and advocate continuous improvement policies of the Information Security Management System, setting standards, benchmarking across the NHS and developing best practice.
- Responsible for developing and implementing a Cyber Security strategy including change control, Root Cause Analysis and error management.

Responsibility for Financial and Physical Resources

- Support the CDO in ensuring budgets are managed and used effectively and promote value for money.
- Will manage a delegated budget
- Identify the physical resources required to deliver an Information Security Management System improvement programme.
- Responsibility for Human Resources
- Responsible in conjunction with the CDO for the recruitment and selection of staff in operational Cyber Security roles.
- Develop and manage awareness programmes in support of key Cyber Security objectives.

- Develop materials that will deliver a robust awareness programme, to all staff within the organisation, for compliance with Regulations (linking in with Organisational Development Team for delivery of same).

Responsibility for Information Resources

- The post holder will be required to regularly produce complex reports and presentations based on a range of information from a variety of sources, audiences will vary but will include the trust Board and sub committees where required.
- Writing and presenting reports to a wide range of groups both internal and external.

Responsibility for Research and Development

- Responsible for developing qualitative and quantitative audits for measuring against professional and national standards and develop action plans for improvement.
- Evaluate published research to inform practice in developing Cyber Security improvements.
- Ensure an evidence based approach to relevant audit/and or evaluation work on all aspects of quality improvement.
- Gather benchmarking

Freedom to Act

- Required to act independently and will decide, within defined areas, how the aims and objectives are best achieved
- Contribute to defining the strategic direction of the organisation in developing improvement
- Responsible for decisions regarding the operational activities in relation to Cyber Security improvement within the trust.
- Responsible for developing a Cyber Security improvement plan for the organisation.
- Manage projects, devise a range of options to overcome problems, analyse the options and take appropriate action to ensure projects are delivered in a timely manner.

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 Service Users 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 Service Users/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 Service Users/clients and staff.
	To maintain the confidentiality of all personal data processed by the

General Data Protection Regulation (GDPR)	organisation in line with the provisions of the 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 Service User contact. Alcohol hand rub before and after Service User 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 Service Users have a duty to contact Occupational Health.

PERSON SPECIFICATION

JOB TITLE:	Chief Information Security Officer
BAND:	8C
DEPARTMENT:	Digital
DIRECTORATE:	Digital
REPORTING TO:	Chief Technology Officer
ACCOUNTABLE TO:	Chief Digital Officer

REQUIREMENTS	**ESSENTIAL**	**DESIRABLE**
EDUCATION & QUALIFICATIONS	• Educated to Masters level or equivalent experience • Management Qualification. • Significant evidence of continued professional development • Formal certification (CISSP, CISM or CRISC) and/or formal training in information security standards and best practice (e.g.: ISO 27001/2, COBIT)	• ITIL Qualification • COBIT
EXPERIENCE & KNOWLEDGE	• Proven and significant leadership experience and/or formal management qualification. • Demonstrated expertise in an IT Security environment • Significant management experience at senior level not necessarily in the NHS • Proven experience of working at a senior level leading and delivering IT Security in a sensitive and complex environment which is undergoing significant change • Experience of delivering presentations to large groups of stakeholders • Demonstrable commitment to partnership working with a range of external organisations • Experience in engaging and influencing stakeholders from diverse backgrounds • Experience of managing and prioritising a budget • Proven track record in IT Secuirty	• Understanding of the role of Data in all aspects of NHS operational activity and 'business' processes. • Demonstrated expertise in a Healthcare environment • Significant management experience at senior level in the NHS
SKILLS AND ABILITIES	• Dynamic personality and the ability to build trusted stakeholder relationships. • Strong external communications skills in a sensitive environment • Ability to prepare and produce concise yet insightful communications for dissemination to senior stakeholders and a broad	• Ability to architect innovative solutions to complex technical problems.

	range of stakeholders as required • Ability to analyse highly complex issues where material is conflicting and drawn from multiple sources (verbal, written and numerical). • Demonstrated capability to act upon incomplete information, using experience to make inferences and decision making • Ability to analyse numerical and written data, assess options and draw appropriate initiatives • Ability to delegate effectively • Demonstrated capabilities to manage own workload and make informed decisions in the absence of required information, working to tight and often changing timescales • Ability to make decisions autonomously, when required, on difficult issues • Working knowledge of Microsoft Office with intermediate keyboard skills. • Ability to provide informative reporting on finances and impact to Board management. • Able to make a connection between their work and the benefit to patients • Consistently reflects on how their work can help and support clinicians and frontline staff deliver better outcomes for patients • Consistently looks to improve what they do, looks for successful tried and tested ways of working, and also seeks out innovation	
PERSONAL QUALITIES	• Works well with others, is positive and helpful, listens, involves, respects and learns from the contribution of others • Values diversity and difference, operates with integrity and openness • Contactable / on-call Cover / call-out in Major Incident in the Trust or Major Digital Project go-lives. • Flexible working at peak periods (particularly project ‘go-live’ or switchover) • Demonstrates professional and personal credibility and integrity and is a respected leader.	
OTHER REQUIREMENTS	• Understanding of Equal Opportunities in the NHS & Equality & Diversity agenda.	