Liverpool University Hospitals
NHS Foundation Trust

Job Description

Job Information		
	Job Title:	Deputy Chief Information Security Officer
	Directorate / Service:	Digital Services/Cyber Security & Information Governance
	AfC Band:	Band 8b
	Professionally Accountable to:	Chief Information Officer (CIO)/Chief Information Security Officer (CISO)
	Responsible to:	Deputy Chief Information Officer (Assurance)
	Base Location:	LUHFT sites
	Job Code:	AS.IT.R0204
	ESR Position Number:	

Job Summary

The role works under the direction and support of the Chief Information Officer and the Deputy Chief Information Officer for Digital Assurance.

The post holder is responsible for leading:-
the day to day proactive management, development and leadership of the Cyber Security and Information Governance teams, to provide the optimum and most cost-effective delivery of Cyber Security (CS) and Information Governance (IG) services and initiatives to the Trust.

To be responsible for the development, implementation and monitoring of information governance and cyber security policy in the Trust

To oversee, and ensure assurance can be provided regarding, the robust protection of Trust and patient data, as well as the protection of infrastructure and assets from malicious activity and actors.

To work collaboratively with NHS England and 3rd party suppliers, including senior managers within Digital Services, in the planning and delivery of the CS and IG agenda across the Trust and act on behalf of the CIO, as required.   Ensuring compliance with the Data Protection and Security Toolkit and other regulatory guidelines.

Providing leadership and a clear vision for implementation of CS and IG as part of the cyber and wider Digital strategy ensuring that effective systems and processes are in place to support the deployment of systems and the modernisation of health services.

To ensure the implementation of the Cyber strategy underpins and aligns with the

Trust's digital strategy and wider Trust strategy and vision.

To lead on IG and CS incident response ensuring appropriate emergency planning, handling, and testing regarding CS and IG incidents, with alignment with wider business continuity and SIRO requirements.

To be an expert and specialist source of advice and guidance on all CS and IG matters to senior stake holders, in their terms, to ensure buy in, support and compliance with the relevant policies and regulatory expectations.

Key responsibilities

- Ensure effective, timely leadership and management of the CS and IG teams in line with Trust and Digital Services expectations.
- Support the CISO in longer term planning, budget control, supplier quote negotiations, business case creation and related procurement decisions and service improvement objectives.
- Maintain knowledge and expertise of the confidentiality, integrity and availability functions associated with applications in general, and specifically the key applications used by the Trust. This should be in the context of ensuring that IG/CS is maintained appropriately across the Trust and to be aware of the daily context in which these packages are used.
- Be responsible for the Trust's Digital Governance related policies, procedures and ensure guidelines are comprehensive and compliant with legislation and current best practice and are implemented effectively across the Trust.
- Ensure the regular review, interpretation and localisation of NHS regulations and other legislative requirements to identify and set the required goals, objectives and standards for the Trust to meet its obligations.
- Provide expert specialist advice to ensure compliance with the requirements of relevant CS and IG legislation including (but not limited to) GDPR/Data Protection Act 2018, NIS, etc.
- Ensure the effective design and specification of associated standards for IG arrangements and reporting of these activities.
- Provide strategic and tactical specialist advice for assessing the adequacy and co-ordinating the implementation of specific controls for new systems, products, or services.
- Ensure a robust system of investigation and reporting on information security incidents as required, including establishing causes and determining appropriate corrective and/or preventive action.
- Ensure the development, improvement and ready availability of expert specialist knowledge on CS and IG to the Trust senior managers and identify and provide guidance and information in relation to related issues.
- To develop and then deliver of a long-term CS and IG plan which considers and aligns with Trust strategy and objectives as well as implementing legislative changes and on-going service adjustments.
- To oversee and provide assurances on the effective and quality delivery of the DSP Toolkit and related work programmes to achieve compliance and maximise adherence levels.
- Development and deliver the Trust's CS and IG annual work programmes including the Data Security and Protection Toolkit, ensuring an integrated programme to maintain and improve organisational performance across the range of related information-handling areas.
- To be able to provide and receive highly complex, sensitive, and contentious

information in the following ways: -

  - To raise the profile of CS and IG across the Trust, supporting high quality and consistent usage of Trust / National applications.
  - Liaise with Trust services and other external organisations to develop and regularly review appropriate information-sharing protocols for information flows across organisational boundaries.
  - To engage with colleagues within the local health community to ensure successful implementation of, and compliance with, legislation, local and National deployments.
  - Provide strategic and tactical advice and guidance on all CS and IG matters, ensuring that all necessary procedures and processes comply with current legislation and making recommendations to ensure that the Trust meets its statutory requirements.
- Analysing and resolving complex and inter-linked CS and IG issues and being able to communicate and obtain buy in from different audiences at all levels.
- Address and resolve issues surrounding CS and IG national initiatives, working with colleagues across the Trust and externally to establish best practice in relation to documents, processes, and data standardisation.
- To liaise and build relationships with PMO and system managers to ensure that digital systems in use within the Trust are accessed appropriately in line with the requirements of internal standards, national and Trust strategic objectives.
- Develop and maintain high level specialist knowledge, underpinned by theory and experience and understanding of key Trust applications, including security and operational functionality, so as to ensure that IG/CS is maintained appropriately across the Trust, but also to enable wider informed involvement and engagement.
- To ensure there is an appropriate and tested CS Incident Management process in place and to oversee and report on required investigations.
- To ensure CS and IG risks are correctly identified in a timely manner and managed throughout their lifecycle. Contribute to the effective operation and improvement of the risk forums, as appropriate.
- Ensure proactive liaison, correct handling, ownership and inclusion of relevant divisional risks with digital aspects within risk management processes. Site managerial dependencies should also be taken into account.
- To oversee and ensure the investigation and mitigation of any breaches highlighted in the compliance audits and report findings back to the appropriate committee.
- Provision of specialist technical advice, guidance, and information to a variety of staff including technical and non-technical staff, and senior managers which may require persuasive, motivational, negotiating and reassurance skills in an informative and understandable manner.
- To lead on the provision of advice and guidance on designs, solutions and services from a CS and IG perspective.
- To chair meetings and manage work packages and workstreams within specific projects and programmes to ensure the correct subject matter expertise is provided in the delivery of the required work.
- To ensure the provision and presentation of CS and IG updates for consideration at relevant forums at all levels, including Board.
- To attend and potentially chair internal and external meetings on behalf of the Deputy CIOs and CIO/CISO when required to represent the Trust CS and IG interests, this may include governance groups, forums, programme meetings

and task and finish groups.

- Ensures the provision of a robust and constantly assessed and improved CS defensive grid.
- To ensure there is an appropriate and tested Information Security Incident Management structure in place with appropriate senior management approval such as the CIO and SIRO.
- To be able to co-ordinate and/or undertake complex and potentially sensitive investigations and arrive at successful outcomes.
- Following process agreed with the CISO/CIO determine and sanction the provision of exceptional security access to meet operational need and/or investigations.
- Planning and managing own time effectively and, within the roles' areas of responsibility, and the time of others to deliver relevant work.
- Plan, deliver and report on risk assessment workshops held at the request of stakeholders on specific risks and issues and using defined methodologies for doing so as appropriate.
- To be responsible for overseeing and ensuring the delivery and quality of all outputs within the CS and IG team and remit.
- To carry out any other duties appropriate to the grade as requested by the Deputy and Chief Information Officer, and CIO/CISO.
- To be part of a Digital on call rota, as required, and ensure a level of oversight over potential Cyber issues out of hours and particularly over extended holidays.
- Accountable for ensuring the provision and maintenance of comprehensive, current and accurate IG/CS information and guidance on the Intranet.
- Regular horizon scanning and knowledge improvement in the constantly evolving areas of CS and IG to ensure prompt reactions to evolving threats or opportunities for improvement, and the ability to provide the most current specialist advice. As part of this there is an expectation of this role to represent the trust at various events and conferences which may include presentations.

Clinical Governance / Quality

The post holder will be expected to adhere to Trust clinical governance and Quality procedures and carry out audits to quantify these as instructed.

Education and training development

The post holder will be required to attend conferences and events to maintain and expand knowledge as well as utilise networking opportunities at all levels.

The post holder will be expected to undertake any further education and training required for this role.

To ensure the assessment, development and delivery of training plans for CS and IG team members and wider Digital Services, as appropriate, that support organisational strategy and objectives.

To devise and deliver formal presentations to senior staff across the Trust to educate and promote Digital Services and CS and IG strategy, policy and processes.

To provide support and leadership to facilitate training on the interpretation and application of CS and IG standards, strategies and policies to all levels of staff within the Trust.

Equality and Diversity

It is the responsibility of every member of staff to understand our equality and diversity commitments and statutory obligations under current equality legislation (the Equality Act 2010) and to:

Act in ways that support equality and diversity and recognises the importance of people's rights in accordance with legislation, policies, procedures and good practice.

Valuing people as individuals and treating everyone with dignity and respect, consideration and without prejudice, respecting diversity and recognising peoples expressed beliefs, preferences and choices in working with others and delivering appropriate services.

- Recognise and report behaviour that undermines equality under Trust policy.
- Be consciously aware of own behaviour and encourage the same levels of behaviour in colleagues.
- Acknowledge others' different perspectives and recognise the diverse needs and experiences of everyone they come into contact with.
- With the support of managers develop an equality and diversity objective through the personal development review process.

Values and Behaviours

We are Caring

We are kind to each other and always show compassion to ourselves and others.

We know we are doing this when:

- We are always **kind** and **compassionate** to ourselves, our patients, families and colleagues;
- We **recognise** and **appreciate** each other, taking pride in working here and our contribution to success;
- We are **professional** and always seek to deliver the best standards of care.

We are Fair

We treat people equitably and value their differences.

We know we are doing this when:

- We value **everyone** for their unique contribution and we embrace diversity;
- We are confident in **speaking up** and we support all our colleagues to do the same;
- We are **open and honest.**

We Are Innovative

We work as a team to continuously improve the way we deliver and transform health care.
We know we are doing this when:

- We **continuously improve** the services we deliver and pioneer new ways of doing things;
- We **learn from mistakes**, striving to ensure we get things right first time;
- We **create and share knowledge** with each other, patients and our professional communities.

Infection Prevention & Control

All staff will always adhere to infection control policies and procedures and carry out role specific duties as per roles and responsibilities.

Confidentiality

Confidentiality/Data Protection regarding all personal information and Trust activity must be always maintained (both in and out of working hours). All staff should ensure that they are familiar with and adhere to all Trust privacy, confidentiality and security policies and procedures. Any breach of confidentiality will be taken seriously, and appropriate disciplinary action taken.

Freedom of Information

In accordance with Freedom of Information and other associated legislation, the Trust may be required to make public recorded information available upon a request, or do this as part of a publication scheme. Please note, that in your public role, your name or job role may be contained in a document that is published in accordance with such legislation.

Management of Risk & Health and Safety

All employees have a duty to take reasonable care to avoid injury to themselves or to others and to co-operate with the Trust in meeting its statutory requirements.

All employees will proactively contribute to the management of risk by identifying hazards in the workplace which have the potential to cause harm, raising issues of concern and risk to the appropriate level.

Safeguarding Children and Vulnerable Adults

All trust employees are required to act in such a way that at all times safeguards the health and well being of children and vulnerable adults. Familiarisation with and adherence to trust Safeguarding policies is an essential requirement of all employees, as is participation in related mandatory/statutory training.

IT Skills

All staff are expected to have or to gain a minimum of basic level IT skills to enable them to use the Trust IT systems to support Trust services and needs. All staff should be familiar with relevant IT systems and security policies and procedures. The post holder is expected to have expert and specialist skills in certain areas.

Records Management

All staff are personally responsible for record keeping. A record is anything that contains information in any medium e.g. paper, tapes, computer information, etc. which have been created or gathered as a result of any NHS activity. All individuals within the Trust are responsible for any records they create or use. Please ensure that records are retained in accordance with the Records Management Policy and are stored in a manner that allows them to be easily located in the event of a Freedom of Information (FOI) request.

Information Quality

All staff must ensure complete and accurate data is collected to the highest standard at all times. Data collection should be supported by adequate documentation and processes should be regularly reviewed. Staff should ensure that processes conform to national standards and are fit for purpose. All staff should comply with the relevant policies in this regard.

Professional Responsibility

Adherence to relevant professional accreditation expectations, industry best practice and LUHFT policy.

Clinical Responsibility

Not a clinical role

Administration Responsibility

- To lead the team in maintaining and improving documentation to support robust governance standards.
- To ensure compliance with all CS and IG principles ensuring the availability of appropriate policy and procedure documents in line with the digital strategy and ensuring processes and structures are maintained.
- Communicate and implement the Trust’s CS and IG Strategy to reflect the Trust’s complex activities and to meet national requirements.
- Ensure appropriate frameworks of control are in place and complied with when sharing confidential and sensitive information with other organisations.
- Ensure regular and effective methods of dissemination and communication around cyber security and information governance, particularly for senior stake holders.
- The principles of Data Protection by Design and Default, and associated IG requirements, are taken into account and used proactively in all relevant initiatives and engagements.
- Ensure all relevant processes and KPIs are monitored proactively and reported in a timely manner where appropriate.
- Accountable for ensuring relevant Intranet information and guidance in the areas of CS and IG are maintained and current.

Research

To maintain an expert knowledge of relevant legislation and national guidance as necessary.

To constantly horizon scan CS and IG developments, and evolving threats and solutions, to ensure the Trust is prepared to proactively react to issues arising and adopt new and best practice standards.

To proactively establish and develop strong external relationships to ensure an awareness of, and a proactive engagement with, wider regional and NHS initiatives.

Accountable for ensuring regular audits / performance monitoring on all aspects of CS and IG are undertaken and that findings are disseminated in the right context/detail to all relevant levels and committees and particularly senior stake holders.

Strategic role

To support the CISO in delivery of the digital strategy with responsibility for ensuring the CS strategy and roadmap is aligned to, and underpins relevant aspects of the Trust Digital strategy

To follow agreed Trust informatics policies and procedures and to liaise closely with the relevant national application project managers to ensure good understanding by users of what their responsibilities are in relation to accessing Trust IT systems.

To be accountable for ensuring monthly and quarterly audits / performance monitoring on all aspects of CS and IG are carried out, ensuring that findings are reported to the appropriate committee and that any recommendations / improvements are implemented.

HR Management

Overarching management of Cyber and IG Teams is a key part of the role, including recruitment, training, professional development, and ensuring the conduct of appraisals, managing and monitoring of annual leave, flexi-time and sickness, mandatory training, health & safety assessments etc.

Involvement in special investigations regarding potential misconduct in the areas of IG and CS, ensuring discrete, robust, suitably justified assessments.

To promote the use of departmental uniforms where provided.

Financial Responsibility

- To ensure the IG and CS budget is managed and utilised effectively.
- To complete bids for external funding to support the IG and Cyber agenda.
- To ensure timesheets are accurate and submitted on time.
- To complete the on line SVL.
- To ensure solutions in use within CS and IG are fit for purpose and cost effective, actively seeking to reduce cost but maintain or, ideally, improve functionality.
- To ensure office supplies are ordered and resources are utilised efficiently
- To contribute to the organisations QEP plan, ensuring efficiency is maximised.
- To ensure data entered on to ORACLE is accurate and up to date
- To identify and create regulatory compliant bids for Cyber related funding to support the Trust’s Cyber and Digital agenda.

Change of Job Description

The duties outlined above are not intended to be exhaustive and may change as the needs of the department alter in line with current agendas. This job description will be subject to periodic review and amendment in accordance with the needs of the Trust.

NHS
Liverpool University Hospitals
NHS Foundation Trust

Person Specification

Job Title:	Deputy Chief Information Security Officer.		
Band	8b	**Job Code:**	AS.IT.R0204

Person Specification				
	Qualifications	**Essential**	**Desirable**	**Assessment**
1	Master's degree level in relevant subject or suitable and equivalent professional accreditations and training CS specific qualifications which may include CISM, CISP, CISA, or other equivalents.	X		
2	Data protection specific qualifications which may include BCS.	X		
3	PRINCE 2 Foundation Certificate or equivalent		X	
4	Evidence of continuous and comprehensive professional development in CS and IG.	X		
	Experience	**Essential**	**Desirable**	**Assessment**
5	Demonstrable extensive experience working in information governance / cyber security	X		
6	Demonstrable experience in engaging successfully with senior and external senior management in a CS and IG context.	X		
7	Experience of managing and progressing **major** change with significant Cyber and Information Security implications or risks.	X		
8	Experience in Leading and managing staff – including performance management, managing sickness absence and disciplinary issues, and managing resources.	X		
9	Excellent IT skills, including keyboard skills and experience of Microsoft Office packages and bespoke databases, preferably including computerised hospital administration systems.	X		
10	Expert experience of writing or implementing NHS security policies and procedures	X		
11	Proven experience of designing and specifying standards for CS and IG based on ISO2700/ISF Standard of Good Practice, etc.		X	
12	Significant experience of implementing and monitoring the DSP Toolkit.	X		
13	Experience of serious and sensitive security incident investigation.	X		
14	Experience of developing plans and delivery of	X		

	strategies and tactical components of cyber security.			
15	Experience of working with, supporting, or implementing security systems within an NHS IM&T environment.	X		
	Knowledge	**Essential**	**Desirable**	**Assessment**
15	Excellent understanding of communication strategies and approaches in relation to sensitive and contentious issues and incidents.	X		
16	An expert understanding of: The Data Protection Act 2018/GDPR Network and information systems (NIS) regulations 2018 DSP Toolkit Cyber Essentials The Access to Health Records Act 1990 The Freedom of Information Act 2000 Confidentiality: The NHS Code of Practice ISO 27001/27002 ISF Standard of Good Practice	X		
17	High level of knowledge of IG and related statutory changes and initiatives.	X		
18	Excellent understanding of CS and IG issues and challenges.	X		
	Skills	**Essential**	**Desirable**	**Assessment**
19	Ability to interpret and apply a range of specialist knowledge and expertise in CS and IG management.	X		
21	The ability to identify, interpret and prioritise key IG/CS issues for senior management and Board review and consideration	X		
22	The ability to analyse and review a range of diverse complex information and produce periodic reports for a wide range of audiences	X		
23	Excellent facilitation, influencing and conflict resolution skills	X		
24	Excellent at verbal and written presentation and communication skills with the confidence to address a variety of internal and external audiences, including senior management internally and externally, and clinicians.	X		
25	Ability to produce effective documentation for audiences ranging from highly technical to non-technical.	X		
26	Excellent negotiation & persuasion skills at senior level and with external bodies/suppliers.	X		
	Other	**Essential**	**Desirable**	**Assessment**
27	Ability to develop good working relationships within a multi-disciplinary team.	X		
28	Ability to plan and organise complex workload under own initiative.	X		
29	Ability to work to tight deadlines and meet targets.	X		
30	Membership of relevant professional bodies such	X		

	as BCS, ISACA, ISC, etc. and have recognised accreditations as above.			