Job Description

Job Title:	Information Security and Compliance Lead
Reports to (job title):	Information Security & Enterprise Architect
Line Manager to:	Information Security Engineer

Job purpose

We are seeking a skilled and motivated Information Security and Compliance Lead to support the strategic and operational delivery of information security and infrastructure controls across our digital estate. Reporting to the Head of Information Security and Enterprise Architecture, this role is responsible for driving compliance with cyber and data protection standards (including DSPT, CE+, and CAF), supporting the secure delivery of IT services, and embedding robust security practices across business-as-usual operations and new service transitions.

Working within the Information Security and Architecture team, the postholder will serve as a senior technical lead across key domains, including cyber assurance, infrastructure security, policy development, and risk mitigation. You will collaborate with technical teams, service management, suppliers, and transformation programmes to deliver a resilient and secure digital environment.

This role is ideal for a technically capable security practitioner or infrastructure expert looking to influence organisation-wide practices while supporting the Head of Information Security in delivering a future-ready, compliant, and secure service model.

Key responsibilities

Security & Infrastructure Assurance

- Support the design, delivery, and monitoring of secure infrastructure services across cloud, on-premises, and hybrid environments.
- Ensure that security controls are applied consistently across networks, servers, endpoints, and backup environments (including Acronis and Barracuda solutions).
- Support the implementation of technical standards and frameworks aligned with NHS DSPT, Cyber Essentials Plus (CE+), and the Cyber Assessment Framework (CAF).
- Collaborate with the Infrastructure and Service Operations teams to deliver secure-by-design solutions.

Job Description

Compliance, Policy & Governance

- Assist in maintaining the Information Security Management System (ISMS), policies, procedures, and risk registers.
- Contribute to internal and external security audits, assessments, and evidence gathering.
- Monitor and report on compliance status, raising risks and recommending mitigations where appropriate.
- Deliver technical security input into supplier reviews, contract renewals, and new technology onboarding.

Incident Response & Risk Management

- Provide senior input into incident management processes, conducting root cause analysis and supporting the Head of Information Security during high-severity events.
- Support business continuity and disaster recovery planning activities across technical teams.
- Maintain security risk documentation and contribute to lessons learned reviews post-incident or transition.

Collaboration & Engagement

- Represent the security function in project and mobilisation forums to ensure new services meet security and compliance standards.
- Support training and awareness programmes for internal technical teams and end users.
- Work closely with Cyber, Infrastructure, Business Systems, and Transformation colleagues to ensure a joined-up approach to digital resilience.

Required Skills & Experience

Essential

- Strong understanding of information and cyber security principles, including access controls, network security, encryption, endpoint protection, and vulnerability management.
- Practical experience supporting compliance with regulatory and best practice frameworks, including:
    - **Data Security and Protection Toolkit (DSPT)**
    - **Cyber Essentials Plus (CE+)**
    - **Cyber Assessment Framework (CAF)** or **ISO 27001**

- Ability to assess security risks, develop mitigation plans, and communicate recommendations to technical and non-technical audiences.
- Familiarity with NHS and public sector data protection responsibilities (e.g. NHS Data Security Standards, GDPR, DSP roles).
- Experience participating in security incident response, post-incident reviews, and technical root cause analysis.
- Knowledge of identity and access management, security logging/monitoring, and asset/information classification.
- Strong documentation skills – able to produce policies, procedures, risk registers, and audit evidence clearly and accurately.
- Experience collaborating with Infrastructure, Digital Transformation, and Service Operations teams to embed secure-by-design principles.
- Confident in engaging with external auditors, suppliers, and governance bodies to represent the organisation's security posture.

Desirable Skills

- Exposure to private cloud environments and related security tooling.
- Experience in security toolsets such as antivirus/EDR, vulnerability scanners, SIEM, or MDM solutions.
- Relevant industry qualifications (e.g. CompTIA Security+, SSCP, CISSP Associate, ISO 27001 Lead Implementer).
- Knowledge of backup and DR security principles (experience with Acronis, Barracuda, or equivalent welcome).

Proposed Job Plan

- Lead the development, maintenance, and implementation of security policies, procedures, and risk registers in alignment with NHS and national frameworks, including DSPT, Cyber Essentials Plus (CE+), and the Cyber Assessment Framework (CAF).
- Coordinate and oversee internal assessments and audits, ensuring timely submission of evidence and continuous improvement of security controls.
- Act as the primary escalation point for cyber and information security matters, including incidents, investigations, and emerging threats.
- Work closely with infrastructure, transformation, and service management teams to embed secure-by-design principles into projects and operational delivery.

- Provide expert guidance and assurance during the mobilisation and transition of new services, ensuring appropriate security controls are in place.
- Represent the Information Security function in governance forums, audits, technical working groups, and operational reviews.
- Develop and deliver staff training, awareness sessions, and briefings to strengthen the organisation's security culture and understanding of risk.
- Maintain visibility across the organisation, engaging directly with clinical, business, and digital teams to identify and address risks, improve understanding, and promote shared responsibility for information security.
- Monitor and report on compliance, threat intelligence, and control effectiveness, providing updates to the Head of Information Security and IMT leadership team.

Education and Skills

Essential:

- Degree-level qualification in Information Security, Cybersecurity, IT Risk, or related subject or demonstrable equivalent experience.
- Evidence of continuing professional development in the field of cyber or information security.

Desirable:

- Recognised cyber/information security qualifications (e.g. CompTIA Security+, SSCP, ISO 27001, CE+ Assessor, CISMP).
- NHS DSPT/CAF training or relevant NHS/public sector compliance experience.

Our values

Our values are our moral compass and core to our DNA. They underpin the way we deliver our services and treat those who use our services.

To many organisations values are just words which don't translate into reality of the day to day but our values flow through everything that we do, they define who we are, what we stand for and set the expectations of our colleagues, communities, customers and partners. They have been defined by our colleagues and have been integral to our journey so far and will be integral to our future as well.

Job Description

We have three values which help us stand out from the crowd, not just because there's only three, but because they are unique to who we are. We care, we think, and we do.

Care	Think	Do
• Inspire	• Challenge	• Accountability
• Understand	• Improve	• Involve
• Communicate	• Learn	• Resilience

Confidentiality and Information Security

As our employee you will be required to uphold the confidentiality of all records held by the company, whether patients/service records or corporate information. This duty lasts indefinitely and will continue after you leave the company's employment.

All information which identifies living individuals in whatever form (paper/pictures, electronic data/images or voice) is covered by the 2018 Data Protection Act and should be managed in accordance with this legislation. This and all other information must be held in line with NHS national standards including the Records Management: NHS Code of Practice , NHS Constitution and HSCIC Code of Practice on Confidential Information and should only be accessed or disclosed lawfully. Monitoring of compliance will be undertaken by the Company. Failure to adhere to Information Governance policies and procedures may result in disciplinary action and, where applicable, criminal prosecution.

Information governance responsibilities

You are responsible for the following key aspects of Information Governance (not an exhaustive list):

- Completion of annual information governance training
- Reading applicable policies and procedures
- Understanding key responsibilities outlined in the Information Governance acceptable usage policies and procedures including NHS mandated encryption requirements
- Ensuring the security and confidentiality of all records and personal information assets
- Maintaining timely and accurate record keeping and where appropriate, in accordance with professional guidelines
- Only using email accounts authorised by us. These should be used in accordance with the Sending and Transferring Information Securely Procedures and Acceptable Use Policies.

- Reporting information governance incidents and near misses on CIRIS or to the appropriate person e.g. line manager, Head of Information Governance, Information Security and Compliance Lead
- Adherence to the clear desk/screen policy
- Only using approved equipment for conducting business

Governance

Clinical governance is a framework through which organisations delivering health and care services are accountable to continuously improving the quality of their services and safeguarding high standards of care by creating an environment in which clinical and other forms of care flourishes. Employees must be aware that clinical governance places a duty on all staff to ensure that the level of care services they deliver to patients is safe and high quality, and that they follow/comply with our policies and procedures.

Registered Health Professional

All staff who are a member of a professional body must comply with standards of professional practice/conduct. It is the post holder's responsibility to ensure they are both familiar with and adhere to these requirements.

Risk Management/Health & Safety

The post holder has a responsibility to themselves and others in relation to managing risk, health and safety and will be required to work within the policies and procedures laid down by the company. Staff are required to observe the Hygiene Code and demonstrate good infection control and hand hygiene.

Employees must be aware of the responsibilities placed on them by the Health & Safety at Work Act (1974) to ensure that the agreed safety procedures are carried out to maintain a safe environment for other employees, patients and visitors. It is essential to observe strict fire and security precautions at all times.

All staff must report accidents, incidents and near misses so that the company can learn from them and improve safety.

Safeguarding Children and Vulnerable Adults Responsibility

We are committed to safeguarding and promoting the welfare of children and adults at risk of harm and expects all employees to share this commitment.

Job Description

Medicines Management Responsibility

Nursing or registered healthcare professionals

Undertake all aspects of medicines management related activities in accordance within the company's medicines policies to ensure the safe, legal and appropriate use of medicines.

Skilled non-registered staff

Undertake all aspects of medicines management related activities in accordance with the company's medicines policy where appropriate training has been given and competencies have been achieved.

Policies and Procedures

All colleagues must comply with the Company Policies and Procedures which can be found on the company intranet.

General

We are committed to serving our community. We aim to make our services exemplary in both clinical and operational aspects. We will show leadership in identifying healthcare needs to which we can respond and in determining the most cost-effective way of doing so.

We recruit competent staff that we support in maintaining and extending their skills in accordance with the needs of the people we serve. We will recognise the commitment from our staff to meeting the needs of our patients.

The company recognises a "non-smoking" policy. Employees are not able to smoke anywhere within the premises or when outside on official business.

Equal Opportunities

It is the company's intention to be an employer of choice and ensure that no job applicants or employees are unfairly disadvantaged on the grounds of gender, disability, race, ethnic origin, colour, age, sexual orientation, religion or belief, trade union membership or any other factors that are not relevant to their capability or potential. To this end, the company has an Equality and Diversity policy and it is the responsibility of each employee to contribute to its success.

Job Description

Flexibility Statement

This job description is not exhaustive and may change as the post develops or changes to align with service needs. Any such changes will be discussed directly between the post holder and their line manager.

Employee signature

Manager signature

care·think·do
WE CHANGE LIVES BY TRANSFORMING HEALTH AND CARE