FCMS (NW) Ltd JOB DESCRIPTION

Post: Information Security Lead

Hours: 37 hours per week, Monday-Friday 9am-5pm (with some evening and weekends required for training delivery across sites and services)

Salary: £29,540 - £33,391 per annum - depending on experience and qualifications

Reports to: The Head of Quality and Risk

Accountable to: Chief Operating Officer

Base: Newfield House, Vicarage Lane, Blackpool, FY4 4EW and will include visits across all sites for training and delivery

Job Summary

Protect. Empower. Lead.
FCMS, a social enterprise for health and wellbeing services, is seeking a dedicated and forward-thinking Information Security Lead to strengthen our information governance and data protection principles across the organisation. We're looking for somebody passionate and proactive to champion a positive and secure culture, who can also provide professional challenge where required with solutions offered or sought out through knowledge, skillset and experience. The post requires the ability to link together a multitude of different compliance elements within a dynamic and fast paced environment; in order to deliver exceptional care to our patients, who are the central focus of all that we do.

This role is a key part of our Quality & Risk Team and central to maintaining the integrity, safety, and resilience of our clinical and corporate systems. This is a pivotal role that blends leadership with hands on influence, empowering staff and managers to embed strong security culture while keeping our digital landscape safe and resilient.

This is more than just your average IT/IG role - this is about safeguarding the trust that underpins every patient interaction!

Key duties And Responsibilities

As our Information Security Lead, you'll be at the forefront of driving a security by design mindset across all teams. You will be responsible for:

Training & Culture: designing and delivering engaging data security training and drive initiatives for staff and managers. You'll be a coach instilling the best practices in a way that sticks, adapting styles as required for the audience, ensuring data security awareness becomes part of everyday working culture.

Information Governance and data protection: design and chair information governance and information asset owner working groups including agenda creation, minutes and action plans and reports. Implementing and overseeing policies and frameworks that ensures data is handled responsibly, legally and securely in line with NHS, ICO and regulatory standards and to coach and support IG champions. Provide assurance and evidence to support NHS DSPT toolkit completion. To manage the audit calendar and implement actions from an IG strategic 12-month focus. To manage the compliance required such as DPIAs, data sharing agreements, information asset registers, day-to-day GDPR queries plus more!

Cyber Security Assurance: conducting regular risk assessments, audits and reviews to identify vulnerabilities and strengthen our defenses whether that is within digital systems, processes or people and environments. To support FCMS with the vision of further developing our digital landscape and the future of health systems, as the world moves into AI and cloud-based products for support with compliance monitoring, reports and recommendations. To support working towards gaining cyber essentials accreditation for any in-house elements outside outsourced ICT services.

Internal ICT oversight: managing relationships with outsourced ICT service providers who provide the ICT infrastructure, networks, cyber division and ICT helpdesk, ensuring ICT services meet security, performance, and user experience expectations for FCMS. You will be the conduit between external ICT services and FCMS to escalate any issues that arises and seek key assurances and KPIs required for data protection and cyber assurances, using frameworks such as the NHSE DSPT and oversee the SLA. You will manage all ICT equipment requests and procurement systems and processes (IT, telephony), you will manage ICT stock delivered, logistics of distribution and installation and work towards streamlining ICT solutions for end user ease. You will maintain and support the development of asset registers. To develop a robust system for policy-based access controls working with external ICT services and internal departments for a robust and secure starter and leaver process to be in place across FCMS. To assist FCMS to fully understand our complex ICT infrastructure, including network perimeters and security architecture – so we can always be on the front foot with setting up any new systems or services across locations for a pro-active approach to further build and support our digital landscape.

Incident Response & Resilience: review data/security breaches or incidents in a timely manner and support teams in any investigations required and produce reports as needed. shape our response protocols and business continuity plans, testing these and supporting services with BCP and incident responses – so we are always ready for the unexpected!

Other duties are required:

This Job Description will be periodically reviewed in the light of developing work requirements. This is an evolving role and therefore, these duties are not exhaustive. The role may change via discussion between the post-holder, line managers and relevant others. The individual in post will be expected to contribute towards that revision. The post holder will be expected to cover the reception desk and administration tasks of Newfield House during sickness and annual leave additionally and carry out any other duties as required and delegated by the Head of Quality and Risk.

General:

To have responsibility for all things under the umbrella of Quality and Risk, maintaining a level of understanding regarding working practices and to always comply with local Safety Policies and Procedures. To observe national and local policies and procedures in respect of: health and safety, Fire and electrical safety, data security and GDPR, counter fraud, Basic Life Support, safeguarding and Infection Control. The post will primarily be based at Newfield House, Blackpool and there is a requirement to travel to other sites and deliver training or help resolve issues within an out of hours setting (evenings and weekends), as required. All mandatory and additional training must be kept up to date as a requirement to this role. Additional training is further required to be undertaken for this post.

What You'll Bring:

• Confidence in training and communicating with non-technical audiences

• Strong knowledge of GDPR, NHS data security requirements, and cyber security principles and able to champion good practices in a way that people can easily understand and apply day-to-day

• Proven experience in information security, data governance, cyber security or a similar field

• A practical understanding of cyber risk management and assurance methodologies

• Ability to work across teams, bridging the gap between IT, compliance, and business functions

• Familiarity with regulatory frameworks (e.g. ISO 27001, GDPR, NCSC, or similar)

• Experience overseeing outsourced IT service providers and liaising with other third parties

• Relevant certifications (e.g. CISSP, CISM, ISO 27001) are a plus—but not essential if your experience shines through

• Attend relevant study/induction days, seminars, courses etc. for individual development and for the benefit of the organisation.

Our key expectations are:

• Self-awareness – Living authentically

• Adaptability- Being ready to adjust depending on the situation Openness – What you see is what you get

• Positivity with a real sense of being able to strive for the impossible Generosity of spirit- Everyday should be an opportunity to act with kindness Ability to have fun – Taking the role seriously, whilst being yourself

Our 'Why': To nurture an environment of inspiration, innovation and disruption so this people in our world receive exceptional healthcare for this generation, and the next.

Values: Our organisational culture is very important to us, so it is vital that the successful candidate lives and breathes complimentary values and behaviours. Our behaviours should be in line with our values which form part of our Company DNA:

➢ **Fun:** People rarely succeed unless they are having fun. Happiness is healthy!

➢ **Awesome:** We aren't here to be average, we're here to be awesome!

➢ **Humble:** We're here to make a difference to the lives of others, NOT to see how important we can become

➢ **Brave:** We challenge the norm. We have the courage to get the difficult jobs done

➢ **Oompf:** We have natural oompf! It's infectious!

➢ **Go-getting:** We are intuitive to changing needs and respond quickly which we do with energy, ideas, and positivity

Come and be a part of our amazing team!

✓ We offer NHS Pension
✓ Cycle to Work Scheme
✓ Career Development Opportunities
✓ Attendance Bonus

✓ Staff Benefit Scheme
✓ Free Tea & Coffee
✓ Eye Care Contributions

Disability Confident Employer
As users of the disability confident scheme, we guarantee to interview all disabled applicants who meet the minimum criteria for the vacancy

DBS - This post is subject to the Rehabilitation of Offenders Act (Exemption Order) 1975 and as such it will be necessary for a submission for Disclosure to be made to the Disclosure and Barring Service (formerly known as CRB) to check for any previous criminal convictions. This will require three forms of valid ID to be produced and verified. The onboarding process is also subject to an Occupational Health check, suitable professional references and eligibility to work in the UK (with the requirement to provide relevant documentation as evidence).

PERSON SPECIFICATION: Information Security Lead

	ESSENTIAL	DESIRABLE
EXPERIENCE	→ Proven experience in information security, data/information governance, cyber security or a similar field and experience of cyber risk management and assurance methodologies → Communicating with non-technical audiences with self-awareness and emotional intelligence, adapting styles as required → Experience of working with IT systems → Experience overseeing outsourced IT service providers and liaising with other third parties → Experience of implementing & monitoring processes → Demonstrated ability to operate in an environment of fast paced change. → Demonstrated ability to meet deadlines, schedules, set goals/objectives → Able to demonstrate effective partnership/team working but also experience of working well on your own initiative. → Problem solving → Ability to work across teams, bridging the gap between stakeholders and functions → Experience working within regulatory data security frameworks (e.g. GDPR)	→ Experience working with Microsoft 365 products → Chairing meetings and confidence in delivering training in a dynamic and engaging way → Experience of working within a healthcare environment. → Line management experience → Experience of Cyber Essentials or ISO 27001 – or have worked towards accreditation → Analysis and report writing skills → Experience of setting up internal reporting systems such as information trackers, performance reports, cascade systems etc. → Experience delivering training and conducting audits → Experience in writing policies and guidance
QUALIFICATIONS	→ 5 GCSE's A* - C including English Language or equivalent training of management or healthcare related qualification. (Experience or qualifications required)	→ Project management → IT, system securities or data qualifications **e.g. CISSP, CISM, ISO 27001**
SKILLS, KNOWLEDGE & COMPETENCIES	→ Strong knowledge of GDPR, NHS data security requirements, information governance and cyber security principles → Extensive knowledge and understanding of information security principles and practices → Attention to detail, Process driven, understanding of own behaviour and skill set, Able to organise own workload → IT skills, Enjoy networking and forming new relationships → Challenge the 'norm', Calm under pressure → *Strong analytical skills. → Knowledge of data protection, GDPR and information governance → Proficient in the use of a PC and computer skills; including the use of email, word processing and spreadsheets. → Excellent communication skills, An elevated level of diligence	→ Negotiation and influencing skills. → An IT whizz → Knowledge of cyber security frameworks in a Healthcare Environment particularly Data Protection, Subject Access Requests, IG Toolkits and DPA/GDPR
SPECIFIC JOB REQUIREMENTS (e.g. physical demands)	→ Prepared to develop and learn new skills → Prepared to be willing to work towards frameworks and Qualifications → Prepared to undertake formal workshop training/qualifications → Manual handling tasks required for taking office/IT deliveries/organising/distributing stock and inventories, organising filing and archive record systems, disposing of old equipment/items	→ A driver's licence, for cross-site working
OTHER	→ Self-motivation → Enthusiasm → Confidentiality → Flexibility → Pragmatism → Initiative → Curious	

The organisation is committed to safeguarding and promoting the welfare of children, young people and vulnerable adults and expects all staff to share this commitment. You will be expected to fulfil your mandatory safeguarding training at the level applicable to this role.

<u>We reserve the right to close this vacancy early if we receive sufficient applications for the role. Therefore, if you are interested, please submit your application as early as possible.</u>

Date Last Updated: 10th April 2025
Updated by: Sarah Evans (Head of Quality and Risk)