|  |
| --- |
| **JOB DESCRIPTION** |
| **Job title:** | IT Cyber Security Lead  |
| **Team/Department:** | IT Operations  |
| **Location:** | Ashford |
| **Hours of work:** | As agreed, and in accordance with the contract of employment |
| **Job title the post holder will report to:** | Director of IT Operations |
| **Job titles reporting to the post holder:** | Non applicable  |
| **Date the role profile was revised:** | August 2023  |
| **JOB PURPOSE**As the IT Cybersecurity Lead, your role is to guide our organization’s cybersecurity endeavours proactively and effectively. You will take a hands-on approach, overseeing critical aspects such as Firewall management, Privileged Access Management (PAM), Security Information and Event Management (SIEM), and Patch management. Your paramount objective is to fortify the integrity and confidentiality of our systems and data. Collaborating closely with the Data Security, Governance, and Protection Team, you will not only meet but also surpass the rigorous standards of the Data Security & Protection Toolkit, Cyber Essentials, and ISO 27001. In partnership with the Director of Operations, you will drive the development and enforcement of our cybersecurity strategy and enforce adoption. |
| **KEY RESPONSIBILITES AND ACCOUNTABILITIES*** Lead a team of cybersecurity professionals responsible for firewall management, PAM, SIEM, and patch management activities.
* Design, implement, and maintain firewall configurations to ensure the organization's network security and protect against unauthorized access.
* Develop and execute a comprehensive PAM strategy, including privileged account discovery, access control, session monitoring, and auditing.
* Configure and manage SIEM solutions to monitor and analyse security events, incidents, and anomalies across systems and networks.
* Oversee infrastructure, server, and end client security patching processes to ensure timely and effective patch deployment.
* Collaborate closely with the Data Security, Governance, and Protection Team to align cybersecurity efforts with Cyber Essentials, ISO 27001, and the Data Security & Protection Toolkit requirements.
* Monitor and analyse CARE CERT alerts, assess their impact, and implement necessary mitigations.
* Investigate and respond to security incidents, including root cause analysis, corrective actions, and documentation.
* Implement and enforce security policies, procedures, and guidelines related to firewall management, PAM, SIEM, patch management, and compliance standards.
* Collaborate with cross-functional teams to integrate security measures into the development and maintenance of systems and applications.
* Conduct regular security assessments, penetration testing, and vulnerability assessments on firewall, PAM, SIEM systems, and patch management processes.
* Provide technical expertise and guidance to the team, including training and mentorship.
* Prepare and present reports on cybersecurity activities, incidents, compliance status, patch management, and performance to senior management.
* Manage relationships with vendors and external partners to enhance cybersecurity capabilities.
 |
| **COMMUNICATION AND KEY WORKING RELATIONSHIPS** The post holder must be able to demonstrate excellent communication and interpersonal skills at all times and build and maintain good working relationships with all stakeholders. |
| **ENVIRONMENT**IC24 is a major not for profit Social Enterprise company currently providing innovative primary care services designed to deliver quality and affordability. IC24 is solutions-focused, providing a comprehensive portfolio of services aimed at improving access and reducing the demand on secondary care services by helping to avoid unnecessary admissions and facilitating early discharge.Going forward, the company is committed to supporting and enabling better integration between health and social care and more effective alliances between partners from different sectors as essential to delivering seamless services. IC24 has considerable experience of working in complex, demographically challenged environments and the Board is keen for the organisation to be proactive in improving standards of care and patient safety, while delivering value for money too in the health economies it which it operates. Critical to this is building strong professional relationships and alliances with third parties; working with them in a way that maximises the benefits of their involvement. |
| **HEALTH AND SAFETY**The post holder will be required to comply with the duties placed on employees of IC24 as set out in the Health and Safety at Work Policy and related procedures. The post holder has a legal obligation to make positive efforts to maintain their own personal safety and that of others by taking reasonable care, carrying out requirements of the law and following recognised codes of practice.All ColleaguesYou have a duty to take care of your own health and safety and that of others who may be affected by your actions at work. You must cooperate with managers and other colleagues to help everyone meet their legal requirements under health and safety law, and not to interfere with or misuse anything that's been provided for your health, safety, or welfare.ManagersYou must ensure you know and understand your responsibilities as defined in our health & safety policies and associated guidance documents. You must identify and assess any risks to people, property, or the environment and ensure all colleagues you have responsibility for, are aware of all our health and safety policies, understand issues arising from risk assessments, site inspections etc. and deal with any associated concerns. You must ensure that all accidents or incidents involving colleagues within your responsibility, are properly reported, and investigated and that regular inspections are undertaken and recorded to eliminate potential hazards and minimise risks. DirectorsYou must ensure that all colleagues and teams within your region and/or department(s), effectively manage health and safety in line with all our health & safety policies and guidance documents. |
| **EQUALITY AND DIVERSITY**IC24 has a Diversity and Inclusion Policy to ensure that no job applicant or employee is discriminated against either directly or indirectly on the grounds of disability, marital status, sex, race, colour, nationality, ethnic or national origin, sexual orientation, age, religion or political opinion, whilst attracting talented recruits and retaining experienced employees.IC24 is committed to promoting equal opportunities and diversity and will keep under review its policies, procedures and practices to ensure that, in addition, all users of its services are treated according to their needs.  |
| **INFORMATION GOVERNANCE** Information is vitally important for the safe clinical management of patient care and the efficient administration of services and resources, including our workforce. Information Governance is a framework to enable IC24 to handle personal and corporate information appropriately.It is the responsibility of our entire workforce, regardless of employment status, to ensure they abide by the requirements of Information Governance as set out in the Data Security & Protection Policy. |
| **SAFEGUARDING CHILDREN AND VULNERABLE ADULTS** IC24 is committed to safeguarding and promoting the welfare of children, young people and vulnerable adults. All colleagues and volunteers are therefore expected to behave in such a way that supports this commitment. You will be responsible for safeguarding the interests of children and adults who you come into contact during your work. To fulfil these duties, you will be required to attend training and development to recognise the signs and symptoms of abuse or individuals at risk, to follow local and national policy relating to safeguarding practice and to report and act on concerns you may have appropriately. |
| **DISCLOSURE AND BARRING SERVICE CHECKS** IC24 will require a DBS check for appropriate roles which is a mandatory requirement and a condition of the employment offer.All posts are assessed on their eligibility for the post holder to be required to undertake a DBS check. For posts that have been assessed as exempt from the provisions of the Rehabilitation of Offenders Act 1974, IC24 will require the post holder to undertake an enhanced DBS check with barred list checks. For posts that have been assessed as being in a position of trust, IC24 will require the post holder to undertake a basic DBS check. This post has been assessed as requiring a basic DBS check.  |
| **REHABILITATION OF OFFENDERS ACT 1974**Some posts have been assessed as being exempt from the provisions of the Rehabilitation of Offenders Act 1974 and in these cases IC24 will require the post holder to disclose all convictions, whether spent or unspent. This post has been assessed as not being exempt from the provisions of the Rehabilitation of Offenders Act 1974; therefore, the post holder is not required to disclose any spent convictions. |
| **PERFORMANCE AND DEVELOPMENT REVIEW**This job description will be used as a basis for conducting an individual Performance and Development Review between the post holder and the manager. |
| **VARIATIONS**This job description describes the main purpose and key responsibilities and accountabilities of the post. The post holder may be required to undertake any additional duties or responsibilities as may reasonably be required.This job description is a guide to the nature and main duties of the post as they currently exist, but it is not intended as a wholly comprehensive or permanent schedule and it is not part of the contract of employment.To reflect changing needs and priorities, some elements of this post may be subject to change and where required, any appropriate communication or consultation with the post holder will be undertaken prior to making any changes.  |

**PERSON SPECIFICATION**

| **Requirements** | **Essential** | **Desirable** | **How identified** |
| --- | --- | --- | --- |
| **Qualifications and Training** | * Qualified to diploma level in the field of either Information Technology or Cyber Security or equivalent education and experience combined.
 | * European Computer Driving Licence or equivalent.
* Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or other relevant cybersecurity certifications.
 | Application |
| **Experience** | * Proven experience in a cybersecurity leadership role, with a strong track record of developing and implementing successful cybersecurity strategies.
* Knowledge of Information Governance and Security and confidentiality issues.
* Knowledge of SIEM management.
* Knowledge of ITIL practices and procedures.
* A good understanding of computers including hardware, networking, and Microsoft software environments.
* Proven appreciation and understanding of the importance of technology for a patient led medical services provider.
* Proven organised approach to work and the ability to multitask.
* Excellent knowledge of Cybersecurity, preferably in a healthcare environment.
* Experience of planning and managing multiple projects.
* Up-to-date and relevant knowledge of developments in cybersecurity.
 | * Experience of working in a senior security position within a large IT Department.
* An understanding of the work undertaken by standards bodies such as BSI, CEN, ISO and W3C.
* Familiarity with PAM systems
 | Application/Interview |
| **Practical skills** | * Ability to follow instructions.
* Self-starter & motivated.
* Ability to work under pressure and to meet tight deadlines.
* Good problem-solving skills.
* Effective time management.
* Experience of working with senior managers or leading professionals.
 | * Ability to research complex technical subjects.
* Emotional resilience and effective stress management.
* Effective communication skills with a variety of media and all colleagues within the company as well as external agencies.
 | Interview |
| **General** | * Proven appreciation and understanding of the importance of technology for a patient led medical services provider.
* Proven organised approach to work and the ability to multitask.
 |  | Application/Interview |