Information & Cyber Security Manager

Role Profile

WHAT I AM ACCOUNTABLE FOR:

Compliance and Standards
•Advise on and evaluate adherence to national and international standards, including ISO27001 and the UK Government Cyber Essentials Scheme.
•Develop and implement action plans to address any compliance shortfalls in collaboration with relevant stakeholders.
Security Operations Management
•Oversee the management of external SOC (SEIM) services and review options to enhance NOC/SOC/SIEM capabilities.
•Manage and resolve all security incidents, ensuring timely mitigation and reporting.
Certification and Compliance
•Supervise and maintain departmental compliance with national certification programs.
•Support the implementation and operation of an information security management system (ISMS) in line with organisational requirements and secure information assets.
Policy and Framework Development
•Prepare, embed, and maintain key elements of the ISMS, including drafting policies, standards, and guidelines.
Project Management
•Lead the delivery of information security projects aligned with the organisation's technical roadmap and priorities.
Risk Management
•Review and assure security documentation such as System Security Plans and Security Assurance Documents.
•Provide advice on cyber risk management for supply chain and managed service providers, including identifying and mitigating risks to ensure regulatory compliance.
Security by Design
•Collaborate with colleagues and the Architectural Practice on 'security by design' principles, ensuring security is integrated into the design and implementation of solutions.
Governance and Strategic Development
•Support the Chair of the Information Security Council or working groups, leading associated planning and strategic initiatives.
Vulnerability Management and Incident Response
•Identify and implement appropriate mitigating actions for vulnerabilities, including conducting security risk assessments.
•Investigate and resolve security breaches, recommending improvements to controls.
Information Governance
•Partner with the Data Protection Officer to ensure security controls align with IG assurance and standards, supporting the Information Assurance Group's compliance efforts.
Audit and Testing
•Conduct and commission information security audits, including infrastructure and system penetration tests, and produce actionable reports.
Training and Awareness
•Develop and deliver information security training programs, awareness campaigns, and induction initiatives to improve security understanding across technical and non-technical staff.
Supplier and Stakeholder Engagement
•Promote best practices in third-party supplier selection concerning information security.
•Manage relationships with key internal and external stakeholders, including executive teams, partners, and service providers.
Community Engagement and Threat Monitoring
•Maintain engagement with external security communities (e.g., regulatory bodies, industry groups, and trusted partners) to stay informed of evolving threats and advancements.
Reporting and Communication
•Effectively communicate insights, findings, and plans to cross-functional teams, management, and stakeholders.
Ad Hoc Responsibilities
•Perform additional duties as directed by the Head of IT and Security, ensuring flexibility to adapt to organisational priorities.

GREEN

Information & Cyber Security Manager

Role Profile

HOW I OPERATE:

Values Led Leadership

- You will believe that everyone has the potential to grow, learn and make choices. Empathetic and mission-driven, you are aligned with the values of our health and social care purpose.
- You will communicate in an authentic and confident way, that blends support and challenge. With a collaborative and inclusive leadership style, and a strong focus on teamwork and knowledge sharing.
- You will embrace change even when it is complex and uncomfortable. Bringing an analytical mindset, you will have a strong attention to detail and a commitment to integrated working.
- You will treat others and those we support as individuals however difficult and challenging.
- You will deliver better outcomes by encouraging ideas and new thinking, facilitating possible improvements and motivating teams.
- You will commit to building a stronger and financially viable Turning Point

WHAT I NEED:

Skills\Knowledge

1.Subject Matter Expertise and knowledge in the field, including best practice standards such as ISO27001, NIST, Cyber essentials and security by design.
2.Working knowledge of the UK GDPR and Data Protection Act 2018
3.A minimum of 8 years' experience in Information & Cyber Security.
4.The ability to influence stakeholders and to determine acceptable solutions.
5.Experience working on complex and business critical Hybrid Multi Cloud systems.
6. Ability to communicate both written and orally, clearly and persuasively, explaining complicated matters simply, tailoring methods/media to suit audience needs and understanding.
7.Ability to clarify, plan and prioritise own work to achieve objectives.
8.Must be self-motivated and be prepared to build process and governance with a strong work ethic.
9.Must take pride in own work, setting and achieving high standards for self and others.
10.Ability to analyse complex problems and propose solutions while satisfying any constraints imposed by the business i.e. resource or time.
11.Ability to consider risks, wider impact of decisions, assessing outcomes and likelihood.
12.Ability to challenge decisions and proposals appropriately to ensure processes are robust.
13.Ability to identify when escalation is required to a more senior level.
14.Demonstrated experience of best practices for organizing, managing and reporting on data.
15.Practical experience with security in AI and automation.
16.Experience creating detailed reports and giving presentations to users and executive management.

GREEN