Information Security Manager

Job Title:	Information Security Manager
Department:	IT Department
Reporting to:	Head of IT
Responsible for (staff):	None
Location:	Redditch
General Purpose of Role:	Responsible for leading, implementing and managing the Information Security Management System

ACCOUNTABILITIES

- Conceptualise and implement an ISO 27001:2013 and GDPR compliant management system.
- Manage the IT Security workstream of initiatives, in order to improve information security within the organisation
- Working with the IT teams, govern day-to-day information security compliance e.g. Malware Protection, Security Incidents, Intrusion Detection Systems, Patch management compliance etc.
- Integrate the new ISMS into the current Arcus Integrated Management System working with the Audit & Governance team.
- Draft and implement Information Security policies throughout the group.
- Build and manage a new Information Security risk management process and integrate into the wider Arcus risk management model.
- Collaborate with key stakeholders and business owners for relevant disciplines, i.e. HR, IT, Audit & Governance, etc. ▪ Provide expert advice and assurance on Information Security related activities to key personnel within the business, including the Board.
- Innovate and introduce new practices, including technology recommendations for Information Security based on industry good practice.
- In conjunction with the Audit & Governance team, conduct internal audits of the business functions with the criteria being: the Arcus management system, industry practice, applicable standards and legislation, and ISO 27001:2013.
- Build and maintain strong relationships with internal personnel and relevant certification, registration and regulatory bodies.
- Create and lead the ongoing awareness and training campaign for Information Security for all Arcus personnel working at all levels, delivering group training sessions where necessary.
- Manage security incidents to closure
- Collaborate on IT risk management
- Coordinate the regular internal and external audit activities including organising participants and managing resulting actions
- Manage internal Security communications program
- Compile and Manage group wide security and compliance metrics reporting
- Work with business and technical functions to align policy to practice and vice versa

KNOWLEDGE AND SKILLS

- Experience of administering security in Server, Desktop and Network environments
- Technical experience of malware protection and data protection technologies
- Project Management, or project lead experience
- Experience implementing and managing an ISO 27001:2013 certified management system.
- Expert and proven working knowledge of ISO 27001:2013 and GDPR.
- Strong knowledge of current Information Security threats and trends.
- Experience working in a multi-client environment.

- Exceptional communicator to all levels of the organisation.
- Experience of training personnel with different competencies.
- Able to work in a fast-paced, challenging environment independently.
- Strong stakeholder management and organisation skills.
- Agile approach to working.
- Experience of project management.
- Certified Information Security Manager (CISM) qualification is desirable.
- ISO 27001:2013 or ISO 9001:2015 internal audit qualification is desirable.
- PRINCE2 Foundation / Practitioner is desirable.
- Knowledge of ISO 9001:2015 is desirable.

VALUES & BEHAVIOURS

Do it SIMPLY:

- Improve every day – provide sustainable, workable and lasting solutions to challenges
- Strive for efficiency – work in an uncomplicated manner, using language and terminology that can be understood by all

Do it WELL:

- Act safely and responsibly – safety first and at the forefront of everything you do
- Excel at customer service – find solutions that meet, where possible exceed expectations

Do it WITH PASSION:

- Perform with pride and purpose – act as a positive role model to others
- Value each other – be open and transparent and respect the views of others

OTHER FACTORS

- The post holder must be able to work flexibly, as determined by business requirements this may involve travelling to other Arcus offices or client's premises