Role Profile

Role Title:	IT Security Manager
Department:	Corporate Resources - IT
Role Purpose:	The IT Security Manager will be responsible for the leadership and effective management of the Information Security strategy. The IT Security Manager will have ownership and day to day management responsibility over the IT Security services and associated policies and processes for Midland Heart. This role will help promote and drive operational excellence in everything we do by enabling organisational efficiency, improving the quality of team collaboration/project outputs and increase awareness of the team within all stakeholder environments, both internal and external. This role will also be responsible for the managing, development and on-going implementation of the organisations information/cyber security strategy and objectives, as well as implementing and improving procedures and processes, awareness and training plans to optimise information security effectiveness. The IT Security Manager will also have ownership and be responsible for aligning the IT team in accordance with the ISO27001 accreditation, as well as ensuring supporting policies and procedures are updated by the relevant parties to be fit for purpose.
Reporting to:	Director of IT
Responsible for:	IT Security Engineer
Disclosure level:	Standard DBS, plus finance background check and watchlist.
Role Level:	Frontline Manager

Key Role Responsibilities	To be an excellence lead and be responsible in managing and leading the end to end IT Security Service, providing 'hands on' assistance, guidance and support to colleagues where required Ownership of the information security risk management framework and working with other disciplines within the IT team.

	Design, create, communicate, implement and continuously improve the IT Security teams processes, strategy and roadmap. Responsible for the management and development of the Information Security technical controls to align to ISO27001 To operate as the lead in all matters relating to Information Security and technical advisor to business stakeholders, ensuring security requirements are considered in new projects and business change. To ensure that all changes to the IT environment – whether they are hardware, software or other system components – comply with the security requirements Achieve desired information security capability maturity by identifying relevant security industry practices and partnering across the organisation to implement improvement projects which mitigate risk and/or improve services Co-ordinate the portfolio of activities and track complex projects involving multiple stakeholders Develop and manage of the IT Security Incident Response plan and associated processes, including investigating and analysing security breaches / non-compliance and 3rd parties in line with legislative and industry best practice. To take responsibility for addressing Information security issues as and when they arise Assist Information Governance in defining the enterprise-wide data protection strategy and drive short and long term efforts to achieve an approach that is consistent with Orbit's risk appetite Attend quarterly Information Security Forum meetings and provide relevant and accurate information to the Group. Work closely with both Information Governance and Project Management Office teams to ensure Information Security best practices are embedded fully within the Project Management Framework Evaluate and test potential security solutions to validate features and functions Promote awareness and enforcement of information security policies and standards

	Perform information security risk assessments and improvement of risk management capabilities Serve as the internal IT Security spokesperson; plan and publish content and deliver internal and external program communications to the appropriate audience through various channels Effectively manage internal, external and cross-functional program and project resources to complete objectives and initiatives Establish relevant metrics and KPIs to communicate status, demonstrate progress and build awareness of information security program performance Respond rapidly and effectively to all IT security incidents, managing them in a professional manner including computer forensics for evidence gathering and preservation. Keep up to date with security trends, threats and control measures. Implement and maintain security initiatives such as Cyber Essential Plus. Develop relationships and engage with industry partners, Security Information Exchanges, and other groups to assess industry advances in technical security technologies and emerging threats – e.g. ICO, Police, CISP and National Cyber Security Centre and security related supplier contracts.

Education, Qualifications and Training	Educated to degree level or equivalent technical level of expertise demonstrated through significant work experience. Hold an Information Security qualification such as CISSP, CISA, CISM, or MSc Information Security.
Knowledge and Experience	Working knowledge of security standards and methodologies such as ISO 27001, COBIT, and ITIL. In-depth knowledge of hardware and software security technologies. Understanding of legislative requirements under General Data Protection Regulation 2016/679, The Data Protection Act, 1998 and the Freedom of Information Act, 2000. An in-depth knowledge of IT security products, systems and applying security best practice.

	Knowledge and experience across multiple technical platforms. Significant experience of managing perimeter security products. Significant experience of Managing Penetration tests and remedial plans. An understanding of Gaining Security Accreditation for the Business such as Cyber Essentials and Cyber Essentials Plus. Experience of Managing 3rd party suppliers. A working knowledge Risk assessment frameworks and mitigation plans. Significant experience of developing and maintaining meaningful IT Security KPI's. Experience of developing, implementing and reviewing Emergency Response plans to ensure business continuity
Role Specific Skills & Behaviours	Excellent presentation skills and the ability to be able to communicate and build strong relationships at all levels. Able to generate your own plans that are aligned to the company's strategy and be able to set and meet deadlines for yourself and others. Able to work co-operatively and productively with customers, other teams, functions and suppliers earning their respect and confidence Commitment to providing quality solutions. Able to develop the skills and competencies of others. Self-starter dedicated to getting results and meeting deadlines. The ability to advise of security requirements and best practice Understanding of and commitment to the principles of Equality and Diversity.