|  |  |  |  |
| --- | --- | --- | --- |
| **Job Title:** | ICT Security Manager | **Date:** | August 2019 |
| **Reporting Line:** | Deputy CIO | **Salary:** | 9 |
| **Team:** | Digital Services | **Business Area:** | Digital Services |

|  |
| --- |
| JOB PURPOSE |
| The ICT Security Manager will proactively lead and manage ICT Security provisions and services for GMCA.  The role holder is responsible for leading on all aspects of corporate ICT Security Policy, procedures and guidance – and will be the subject matter expert for the organisation. Reporting directly into the Deputy CIO this role will be part of the Digital Services leadership and management team.  As the organisational specialist in this field the role holder will be required to advice and influence strategic decision making at all levels within the organisation, to specialists and non-specialists and to board level members – ensuring continuous improvement and compliance against legal and ethical standards. |

|  |
| --- |
| **KEY RELATIONSHIPS** |
| * Digital Services Team * Information Governance Team * Senior Management Team * Corporate Leadership Team * Leadership Team * Extended Leadership team * Pan GM collaboration networks * GM Local Authorities |

|  |
| --- |
| **KEY RESPONSIBILITIES** |
| * Leads on all aspects of corporate ICT Security policy, procedures and guidance, including; cloud, network, encryption, anti-virus, devices, datacentres, physical security, influences the ICT Teams working with these ICT specialisms. * Leads on Risk Management for the ICT department, advising on the ICT Risk Register for aspects associated with cyber security, and works closely with risk owners and the risk processes * Develops and manages an Information Security Assurance program, reviewed quarterly and provides responses to Internal and External Auditing services. * Leads on ICT Security testing including defining penetration testing, partnering with external organisations to ensure the ICT physical and virtual security of the GMCA technical infrastructure. * Lead on planning and response to ICT-related Disaster Recovery and Business Continuity matters, responding immediately to security-related incidents, spearheading vulnerability audits, forensic investigations and mitigation procedures, and provide a thorough post-event analysis * Advise within the department and across the organisation on current and potential threats, and mitigation, including solution design that supports information legislation compliance i.e. Data Protection legislation * Lead and institute organization-wide training and awareness in security protocols, policies and procedures * Lead and develop - as the subject matter expert - all ICT Security policies, procedures and resources, to ensure the consistent and effective design of ICT security services and performance metrics. * Providing technical security advice to support design, procurement and installation of technology to enhance information security and ensure information legislation compliance. * Manage projects and initiatives ensuring that the standard project management methodology is properly utilised. Provide opportunities for staff by encouraging cross-directorate and matrix working, ensuring that project team members understand the desired outcomes of the project and the roles that they each play in delivering them.   **General**   * Effectively plan and manage financial resources in own area of responsibility based on an in depth understanding and interpretation of both financial and management information data, in order to deliver public value. * Identify and contribute to upskilling opportunities for colleagues within and beyond the directorate * Build effective relationships with clients, customers and key stakeholders. * Where required, coach system users to develop effective skills, and provide guidance and support on the use of systems and tools to enable them to undertake their roles. * Review key performance indicators to identify and address issues arising, spot trends and take appropriate action to learn, share and improve. * Seek feedback and elicit wider priorities to support and enable colleagues to meet the needs of the organisation. * Proactively contribute to continuous improvement of systems and processes to ensure procedures, policies and guidance are updated in line with legislative and social changes. * Develop on-going communication and engagement channels and methods to keep the wider directorate team, internal and external customers up to date * Provide positive challenge to colleagues across the organisation in considering how things can be done better and more effectively. * Communicate effectively to ensure all relevant stakeholders are informed and up to date with relevant information, statuses and progress. * Produce, monitor and input accurate information into the relevant systems ensuring all data is up to date and inputted in a timely manner * Accurately prepare documentation, communications and information including letters, emails, contracts and records. * The role holder will work collaboratively across the directorate engaging with internal customers, clients and stakeholders to provide internal focused consultancy, support and guidance.   **NB:** This list of duties and responsibilities is by no means exhaustive, and the post holder may be required to undertake other relevant and appropriate duties as required. |
|  |

|  |
| --- |
| **KNOWLEDGE, SKILLS AND EXPERIENCE** |
| **Education, qualifications and associations**  **Essential**   * Holds or working towards security certification i.e. CISSP, CISM /ISO 27001 * Educated to degree level in relevant area or equivalent or 5 years plus senior-level experience in a relevant environment * Relevant professional qualification, membership of a relevant professional body. * Evidence of continuous professional development * Understanding of ITIL and PRINCE2 basic principles   **Desirable**   * Working towards ITIL Certificate and PRINCE2 * Management qualification e.g. Business Administration   **Essential knowledge and experience**   * Experience in managing Information Security Management e.g. ISO/IEC 27001 * Sound understanding of risk management methodology and information security techniques * Technical experience across a range of solutions and platforms in the Public Sector arena. * Working knowledge of project management methodologies and an ability to apply these in practice, and experience of successfully managing complex projects from inception to completion * Experience of analysing and interpreting complex information and communicating it appropriately to a range of stakeholders. * Must have the proven ability to work under pressure and without direct supervision on many tasks, prioritising to meet deadlines and be able to manage the workload to achieve set targets. * Experience of dealing with external suppliers and managing issues from inception to conclusion with third party organisations. * Experience as an ICT Security subject matter expert leading ICT Security design for a large public service organisation * Experience of designing and leading on all aspects of ICT Security policy, including cloud, network, application, encryption, anti-virus, devices, datacentres, physical security and similar * Knowledge of horizon-scanning and innovative mitigation of risk across the ICT infrastructure * Strong technical understanding of Microsoft on-premise and cloud-technologies (including; Azure, SharePoint, Dynamics and Office 365) from an ICT Security standpoint * Network configuration and security: infrastructure, application, virtualisation * DNS hosting and network configuration * General principles of mobile device management, configuration and encryption technologies * Produce and maintain documentation - policies, procedures and guidance as appropriate. * Experience of working at a senior level, advising at corporate leadership level on ICT Security matters for a large public sector organisation. * Experience of maintain compliance with information legislation. * Experience of setting and agreeing security objectives for the organisation and monitor security performance, including the timely investigation of security incidents and events, analysis of root cause of problems and delivering security by design.   **Desirable knowledge and experience**   * Experience in implementing Information Security Management Systems including ISO/IEC 27001:in the ICT Department of a Public Sector Organisation or a Medium/Large Private Sector Organisation * Experience in a key role that influences, contributes to, or advises on the strategic direction taken on the resilience and security of a medium sized organisation (ideally in the local government arena) * Demonstrable experience of successful project management of a new technology, system or a major upgrade of a corporate system impacting on a wide number of users across the Service   **Skills & Behaviours**  **Essential Skills & Behaviours**   * Well-developed verbal and written communication skills, including report-writing, presentation and facilitation, able to advise / influence at all levels; explaining technical detail to a non-technical audience including to senior and executive leadership. * Ability to collate, critically appraise and present information from a range of sources using excellent analytical skills. * Ability to build strong and trusting relationships with clients, customers and colleagues, including senior leaders * Self-motivated with an ability to prioritise and organise work effectively to meet deadlines. * Ability to manage the effective implementation of projects. * Ability to generate new ideas, alternative options and develop realistic and practical solutions. * Excellent ICT skills - IT Literacy - experience with Microsoft Windows and the Office productivity suite * Clear focus on delivering positive outcomes and acting as a role model for the directorate * Able to work flexibly and independently, covering other areas of the department as required * Self-motivation and ability to deal with a demanding workload and deliver consistently to deadlines * Ability to work flexibly and creatively as part of an effective team * Commitment to high standards of customer care and public service * Strong management and leadership skills * Requirement to travel outside the county to attend meetings etc. when required may include overnight stay. * Occasional requirement to attend residential training courses * To be willing to work flexibly as occasional evening and weekend working may be required * Willingness and ability to travel across the county when required, within a reasonable time to meet the role demands (individuals providing their own vehicle for use will be eligible for casual car user rate |

**Corporate Duties**

Avoid any behaviour which discriminates against your fellow employees, or potential employees on the grounds of their sex, sexual orientation, marital status, race, religion, creed, colour, nationality, ethnic origin or disability.

Safeguard at all times confidentiality of information relating to staff and pensioners.

Refrain from smoking in any areas of Service premises.

Behave in a manner that ensures the security of property and resources.

Abide by all relevant Service Policies and Procedures.

**Records Management/ Data Protection -** As an employee of the GMCA, you have a legal responsibility for all records (including employee health, financial, personal and administrative) that you gather or use as part of your work with the Service. The records may be paper, electronic, audio or videotapes. You must consult your manager if you have any doubt as to the correct management of the records with which you work.

**Confidentiality and Information Security -** As a GMCA employee you are required to uphold the confidentiality of all records held by the GMCA, whether employee records or GMCA information. This duty lasts indefinitely and will continue after you leave the GMCA employment. All employees must maintain confidentiality and abide by the Data Protection Act.

**Data Quality -** All staff are personally responsiblefor the quality of data entered by themselves, or on their behalf, on GMCAs computerised systems or manual records (paper records) and must ensure that such data is entered accurately and, in a timely manner, to ensure high standards of data quality in accordance with Departmental protocols.

To ensure data is handled in a secure manner protecting the confidentiality of any personal data held in meeting the requirements of the Data Protection Act.

**Health and Safety -** All employees of GMCA have a statutory duty of care for their own personal safety and that of others who may be affected by their acts or omissions. Employees are required to co-operate with management to enable GMCA to meet its own legal duties and to report any circumstances that may compromise the health, safety and welfare of those affected by the Service’s undertakings.

**Service Policies -** All GMCA employees must observe and adhere to the provisions outlined in these policies.

**Equal Opportunities -** GMCA provides a range of services and employment opportunities for a diverse population. As a GMCA employee you are expected to treat all employees / partners / members of the public and work colleagues with dignity and respect irrespective of their background