

**Regulation and Technical**

**PG6683**

**Post Specification**

|  |  |
| --- | --- |
| **Date** | **19/05/2017** |
| **Post Title** | Information Security Officer |
| **Role Profile** | **RT12** |
| **Final Grade** | **Grade 12** |

**To be read in conjunction with your role profile**

|  |
| --- |
| **Service Area (brief description)** |
| Business Service - ICT  |
| **Purpose of this post**  |
| * To assist in bringing the organisation’s information security risks under explicit management control.
* To supporting the organisation with Information Security compliance advice, security planning and other related issues.
* To support the organisation’s nominated Senior Information Risk Owner (SIRO) and Information Security Manager by making appropriate policy and operational recommendations and reporting on potential and actual breaches.
 |
| **Key job specific accountabilities**  |
| * Provide expert advice to the organisation on information risk analysis/management.
* Review and develop the Information Security policies as required and at least annually.
* Develop and implement Information Security training programmes in line with business need and liaise with Learning & Development to design and manage the delivery of courses.
* As required by the Information Security Manager and in conjunction with the Information Governance Manager, investigate suspected and actual breaches of security and undertake reporting/remedial action, ensuring that the details are correctly recorded in the appropriate logs.
* On an ongoing basis assess the organisation’s Information Security measures and departmental process and procedures to ensure that they meet current Information Security requirements and conform to the organisation’s Information Security policies, reporting any deficiencies or anomalies to the Information Security Manager and making recommendations as to remedial actions.
* Establish and maintain a register of information asset owners for sets of information and educate them on their responsibilities and provide ongoing support.
* Develop and implement a mechanism for defining and maintaining information flow maps within the organisation, and between the organisation and partner organisations - providing advice where necessary.
* Ensure that registers are maintained for Risk, Issue and Change Information Security.
* Challenge the organisation’s Information Security effectiveness and report regularly to the Information Security Manager.
* Maintain currency with the Information Security and Cyber landscape, threat responses and available Information Security technologies and provide appropriate advice and support to the organisation.
* Provide advice in response to Information Security audit findings and recommendations and take appropriate action as required by the Information Security Manager.
* Provide expert advice, support and challenge to Incident Management.
* Provide expert Information Security advice within the Change Management process.
* Provide expert advice on, implement and document the Information Security elements of external compliance protocols (e.g. PSN, IG Toolkit, PCI DSS).
* Be the first point of contact for operational Information Security requests and make balanced Information Security decisions based on risk management.
* Liaise with stakeholders, third parties and suppliers on Information Security matters.
* Participate in the wider Information Security community e.g. NW WARP.
* Deputise for the Information Security Manager as required.

Please note annual targets will be discussed during the appraisal process. |
| **Key facts and figures of the post** |
| Budget responsibilities | * N/A
 |
| Staff management responsibilities | * N/A
 |
| Other | * N/A
 |
| **Post Specific - Qualifications, knowledge, experience and expertise** |
| * NVQ level 4 or demonstrable equivalent.
* Ideally hold a degree and/or relevant professional qualification.
* Ideally will have completed formal training in Information and Cyber Security (e.g. CISSP).
* Thorough understanding of and experience of working with relevant Information Security legislative requirements, protocols and standards.
* Public Sector Information sharing protocols and strategies.
* Working in areas operating within a risk management framework.
* Working in change agendas that impact on an organisation’s Information Security agenda.
* Operate within a performance management framework.
* Ability to liaise with staff and managers at all levels and across directorates.
* Ability to liaise with stakeholders and Information Security solution providers.
* Assess potential change initiatives and contribute to solutions that are risk appropriate.
* Develop solutions that place a balanced emphasis on the end user experience and Information Security assurances.
* Ability to prioritise own tasks and work independently without supervision.
* Produce clear action planning and reports.
* To have a solution focused outlook and a ‘can do’ approach.
 |
| **Job working circumstances (only include if additional JWCs apply)** |
| **Emotional demands** | * Minimal emotional demand
 |
| **Physical demands** | * No demand for lifting heavy and/or bulky equipment, and/or working in awkward or confined spaces
 |
| **Working conditions** | * No exposure to adverse weather, occasional working with adverse temperature and/or noise, normal levels of adverse people behaviour
 |
| Other Factors |
|  |