

JOB DESCRIPTION AND PERSON SPECIFICATION

JOB TITLE: Information Security Manager

RESPONSIBLE TO: Information Governance Group Manager

GRADE: E

HOURS: 37

(This post requires SC security clearance)

PURPOSE OF POST

ICO must be a model of good practice for the legislation which it regulates and is committed to continuous improvement in this area.

The post holder will take the lead and provide a focal point for security and information risk matters.

The post holder will be responsible for plans to develop and improve information security at the ICO.

KEY RESPONSIBILITIES

- To develop and maintain the information security policy and accompanying standards, procedures and guidance
- To develop and deliver a programme of planned compliance reviews and ensure any gaps are addressed
- To promote security awareness by developing and implementing a security awareness and training programme
- To investigate suspected and actual security incidents in accordance with the security incident management standard, produce reports with recommendations and ensure any remedial action is taken
- Produce reports for the Information Governance Steering Group (IGSG), Information Asset Owners (IAOs) and the Senior Information Risk Owner (SIRO) as required
- Respond to enquiries from staff and provide security advice as required

- Work with internal stakeholders to develop relationships to help promote and improve information security and provide security advice on procurements, projects and new initiatives as required
- Work with external stakeholders for example MOJ, CESG, internal auditors and our Accreditor as required
- Coordinate the development of the Risk Management Accreditation Set (RMADS) and the annual accreditation processes
- Provide line management for the Information Governance Officer
- Provide input to the wider development of the information governance strategy and business planning process
- Maintain currency with emerging security trends, risks, new guidance or standards (internal and external) and security enhancing technologies

PERSON SPECIFICATION

	Criteria	How Assessed
Education and Qualification	Educated to degree level	Application
	Or	
Work Experience	Substantial work experience at a level demonstrating graduate ability	Application and interview
Knowledge, skills and ability	Understanding of, and practical experience of applying the Data Protection Act, the Freedom of Information Act and other related legislation, standards and codes of practice	Application and interview
	A good working knowledge of	Application and interview

	<p>information security including ISO/IEC 27001 Information Security Management Standard</p> <p>Ability to lead and deliver change and contribute to culture change successfully</p> <p>Ability to influence at senior levels on matters relating to security and information risk</p> <p>Good verbal and written communication skills and able to communicate effectively at all levels</p> <p>Ability to manage time and priorities appropriately</p> <p>Good working knowledge of information risk analysis/management</p> <p>Positive attitude towards learning and development demonstrated by a record of continuing professional development</p>	<p>Application and interview</p> <p>Application and interview</p> <p>Application and presentation</p> <p>Application and interview</p> <p>Application and interview</p> <p>Application and interview</p>
--	---	--