**Job Description**

Job descriptions should be no more than four pages when complete. In line with the Welsh Language Act you need to consider if welsh is required for the role and complete as necessary.

**Where you are amending an existing job description you must make the changes using Track Changes.**

Once you have decided what role you require within your team / department structure, you need to articulate this into a job description. This needs to be a specific description of the role, including the responsibilities that the job-holder will carry out as well as what qualifications and skills they will require to fulfil the role. Please note: job description should not be based on an individual but on the role the business requires.

Job descriptions must be accurate and created before the recruitment process.

|  |
| --- |
| A Post Details |
| Job Title: Information Security Officer | Grade: B002Only state the grade if this an existing role otherwise leave blank |
| Department: Information Management | Division: A  |
| Reports to: Information Security Manager | Contract Type: Permanent |
| Level of Vetting:Security Check | Numbers in Post: 3 |
| Welsh language required No |
| B Purpose of the Post |
| To establish and maintain policy and guidance to ensure the confidentiality, integrity and availability of information assets in BTP. To undertake detailed risk assessments and provide subject matter expertise when proposing detailed technical control measures and mitigations to ensure BTP data is managed in accordance with the Force risk appetite. To comply with legislation including data protection, privacy by design, ensuring compliance with national policies and standards from the Police Digital Services (PDS) and the National Management Centre (NMC), in particular international standards such as National Institute of Standards and Technology (NIST), ISO27001 and any other applicable standards. The ISO will act as Force Assurer to ensure that all business critical and essential policing systems are assured and compliant with the standards required by PDS, Community Security Policy (CSP), HMG Security Policy Framework, National Cyber Security Centre (NCSC) and Data Protection Act (DPA) / General Data Protection Regulation (GDPR). Responsibilities include undertaking of technically complex and detailed risk assessments and compiling formal Risk Assessment and Assurance Reports for the approval by the Information Security Manager and ultimately the Senior Information Risk Owner (SIRO).  |
| C Dimensions of the Post |
| The decisions and advice given by the post holder could have an impact on both the expenditure, resourcing and senior decision making on projects/department. |

|  |
| --- |
| D Principal Accountabilities |
| Develops and maintains a suite of policies and guidance to create a governance framework to provide appropriate levels of security of information in BTP. This includes interpreting national policies and Police Digital Services (PDS) policy and guidance to provide a policy framework supporting best practice for safeguarding information systems, assets and our people.Provides advice and guidance across all areas of the business on a daily basis, which includes advice on appropriate physical and technical control measures, as well as relevant policy or operating procedures and best practice on how to safeguard BTP information assets, generally termed as information security BAU activity to safeguard the reputation of BTP.Ensures adoption of and adherence to detailed, technical information assurance standards, strategies, policies and guidance across Force initiatives, processes, and projects involving BTP’s technology assets, systems and information assets, working alongside Cyber Security for comprehensive assurance across the business.Plans, organises, and conducts information assurance activities and accreditation of services across business areas and the supply chain, including national connections, Police Secure Network (PSN) and other codes of connection. To include carrying out risk management activities with varying degrees of complexities within a specific function, technical area or project, often within short timescales. Working with others such as Cyber Security, Digital Policing and other technology functions.Undertaking due diligence to identify risk and vulnerabilities for a wide range of detailed and complex technical projects, benefitting the organisation in terms of value for money, supporting the Force on the Move Strategy and objectives, as well as ensuring compliance with its legal obligations. Assesses the impact of the risk to vulnerabilities from a range of threat actors by conducting detailed security risk assessments and business impact analysis. Which develops mitigation strategies and control measures to manage risks to an acceptable level in line with the force’s risk appetite, which are reported together with recommendations for action through to the Head of Information Management. Responsible for investigation, co-ordination and reporting on information data breaches and information security incidents, some of which may be complex in nature, including the appropriate triaging of all incidents, focusing on containment and recovery ensuring preventative action is taken to minimise the risk of a reoccurrence and reputational damage to the Force.Liaise with the Data Protection Officer (DPO) to make informed decisions on reporting to the Information Commissioner’s Office (ICO) and attending Gold Groups as required.Conduct detailed analysis of incidents and trends to affect organisational learning, reporting both nationally to PDS and internally to Force Information and Assurance Boards.Carry out technical and physical information security audits i.e., Police Assured Security Facilities (PASF) of 3rd party suppliers and compliance checks across all business activities to determine effective controls are maintained including the ability to undertake Information Assurance work for other Forces.To liaise and support Force Information Asset Owners (IAO) across the business to actively maintain the Forces Information Asset Register (IAR) in compliance with DPA and General Data Protection Regulations (GDPR).To participate in programme and project board meetings for a ‘Force on the Move’ transformations programme and other change initiatives, leading on the implementation and assurance of project deliverables, potentially impacting budget and resources.Providing advice and awareness throughout BTP on cyber threats and information security related matters as well as advising on wider information assurance training.Support the Force Information Security Manager to ensure accreditation to the Police Secure Network for Policing (PSNP) and other Home Office Accreditations, such as Airwave is approved and maintained.  |
| E Decision Making |
| Ability to work under own initiative. Uses professional discretion and decision-making methodology in risk-assessing and identifying control measures or solutions to maintain the confidentiality, integrity and availability of all BTP information assets.The decisions made will have a direct impact on overall substantial level of spend on projects, with a focus on value for money whilst influencing best working practices across the business.Determines when issues should be escalated to a higher level. |
| F Contact with Others  |
| InternalEngagement with BTP Users, IAO’s, Heads of Department, senior officers and police staff, and departments such as Cyber Security, Technology and Digital Policing.ExternalPolice Digital Services (PDS), National Management Centre (NMC), National Cyber Security Centre (NCSC), Government Communication Headquarters (GCHQ), Centre for the Protection of National Infrastructure (CPNI) and other Forces, 3rd party suppliers and technology partners and consultants. |
| G Essential Criteria  |
| Qualifications and Training:  |
| Educated to a minimum 5 GCSE grades A-C or equivalent qualification including English and Mathematics The post requires significant and relevant experience in Information Security and Risk Management ideally within the policing community. This includes providing information assurance support to technology projects, assessing and controlling risks, and liaising with business partners at all levels to provide assurance.Must be able to hold or attain a recognised Information Security qualification (such as BCS Certificate in Information Security Management Principles) or equivalent security qualification.Trained in Risk Management Concepts & Accreditation Processes. |
| Experience:Excellent interpersonal and communication skills in Welsh No |
| Able to demonstrate a detailed understanding of Information Security concepts and practices concerned with maintaining the confidentiality, integrity, and availability of information.Establishing, developing and delivering IA processes and procedures within a large organisation. Interpreting key legislative requirements and National and International Information Security Standards, documenting them in local policies and procedures.Investigating complex Information Security incidents and providing recommendations to senior management and the Information Security Manager to mitigate risk.Undertaking detailed risk assessments, audits and accreditation activities, and preparing detailed reports, idendifying vulnerabilities and offer recommendations and solutions. |
| Skills:Excellent interpersonal and communication skills in Welsh No |
| Work under own initiative, independently, as well as working as part of a team.Must evidence mental agility and ability to solve complex issues when tasked with new projects using experience and knowledge of information assurance standards to successfully deliver outcomes within tight timescales.Work to tight deadlines, on time and to required standard, while managing own resources in order to respond to changing demands and deliver efficient follow-ups.Demonstrate impactful communication skills (oral, written and presentation) in both formal and informal settings, including the ability to explain complex issues to broad audiences that will influence decision making across the business.Demonstrate skills in engaging and working with a range of internal and external stakeholders.Ability to work within the business to understand and interpret Information Security risks and control measures.Must be able to give and receive constructive feedback, focusing on practical improvement. Strong IT skills, including working knowledge of O365, including Microsoft Word, Excel, and PowerPoint.Can take the initiative to advance own skills and maintain awareness, while identifying and managing development opportunities in area of responsibility.  |
| Knowledge: |
| Knowledge of risk management, accreditation and assurance methods.In depth understanding and practical knowledge of current Information Security Management standards and best practice, including HMG Security Policy Framework, PSN Code of Connection, National Institute of Standards and Technology ISO27001 and any other applicable standards.Sound understanding and knowledge of relevant statutory obligations, including Data Protection Act / GDPR and the Government Security Classifications.  |
| Desirable criteria:  |
| Qualified in CPNI Protective Security in the Critical National Infrastructure (CNI) and other relevant modules.Member of the Chartered Institute for Information Security (CIIS) or member of the Chartered Institute for IT (BCS).Cerified ISO27001 Internal Auditor or similar.Knowledge of the Freedom of Information Act 2000.Knowledge and understanding of the technical, human resource, procurement, project and physical security issues that impact upon information security. |
| H Additional Information |
|  |
| For Panel to complete only:Line Manager Approval: (this is only signed off when the line manager has approved the final version)Panel Approval: (this will only be signed off once the job has gone through the Job Evaluation Panel)Date:Click or tap to enter a date. |

Email the Job Evaluation submission form together with supporting documentation (organisational charts, job descriptions) to **People & Culture Policy & Reward inbox**

You will be advised of a panel date following receipt of the submission