Job Title: IT Security Analyst	
Job Evaluation Number	B965

JOB DESCRIPTION

Job Title: IT Security Analyst	**Location:** Kidlington or Southampton with travel
Job Family: ICT	**Role Profile Title:** BB3 Police Staff
Reports To: IT Security Officer	**Band level:** 3S
Staff Responsibilities (direct line management of): Nil	

a. **OVERALL PURPOSE OF THE ROLE**: Defines the role, put simply, why it exists.

***The overall purpose of the role is to*:** Monitor technical controls, detect and respond to IT security incidents in support of the ISO/IEC 27001 Information Security Management System (ISMS). Providing IT Security advice to Technical Architects and Project Managers.

b. **KEY ACCOUNTABILITY AREAS**: Define the important aspect of the role for which the job holder is responsible for results or outcomes.

The key result areas in the role are as follows:
1. Provide expert Security Architecture advice to Technical Architects and Project Managers to ensure implementation of pragmatic, proportionate, cost-effective cyber security controls. Identify technical information risks and propose mitigation to management. Identify new and emerging technologies and evaluate how these can be used securely to improve communication. Also, identify and propose secure implementation of products or technologies which may be consumer rather than business focused (such as smartphones).
2. Provide the initial response and management of IT Security incidents and escalating to the IT Security Officer as appropriate. Assist with the Protective Monitoring of technical security controls and respond appropriately to IT security incidents, escalating to the IT Security Officer as appropriate. Identify new and emerging cyber threats and propose mitigations and countermeasures to emerging cyber threats.
3. Contribute to the oversight and monitoring of Administrative (Sys Admin) access control ensuring that joiners, leavers and movers access is appropriately maintained.
4. Maintain contact with security authorities to ensure that security warnings/advisories are appropriately monitored and acted upon to ensure that the Forces' information remains secure against external and internal threats. Represent the IT Security Officer at local, regional and national meetings in relation to information security and assurance, as required, and provide peer support and assistance when appropriate.
5. Work with the forces' auditors and accreditors on the audits of IT security controls to ensure the quality and accuracy of the audit and also ensure that actions arising from the audit are completed as appropriate (including ITHC remedial actions).
6. Assist with change requests that relate to security enforcing functions to ensure compliance with forces' IT Security policies.
7. Assist in the provision of advice and guidance on IT security to members of the department and within the business areas to ensure all stakeholders have a clear understanding of IT Security controls and processes. Cultivate relationships with stakeholders in order to raise awareness and proactively contribute to improving the two forces' adherence to information security standards.
8. Assist with proactive scanning of future changes to technology, policy, process and legislation to identify and assess any information risks to the organisation and suggest any technical mitigation. Develop, implement and maintain technical security policies in support of the ISMS.

c. **DIMENSIONS**: Include matters as key result areas that make the greatest demands on the role holder, seasonal pressures, items processed, the number of customers and/or level of authority to make financial decisions or commit other resources

Further Comments:
Work across forces' areas to provide resilience as required.
Vetted to the appropriate level to identify and handle sensitive, personal and classified information in accordance with recognised Information Management standards and legislation.
Must be able to travel regularly across forces' areas and attend occasional regional and national meetings.
Must be delivery focused and able to appreciate Information Security matters in a wider business context, enabling the business to meet its objectives. Must have a customer service ethos and be an effective advocate for Information Security.
Provide advice and guidance that is aligned to current HMG and police policies (such as Security Policy Framework and ISO/IEC 27001) and supports new technologies such as Cloud and Mobile technologies.

d. **CHARACTERISTICS OF THE ROLE**

Expertise: Concerned with the level of administrative, professional and/or technical expertise (knowledge and skills) needed to perform the role effectively; may be acquired through experience, specialised training, and/or professional or specialist education and training.

The knowledge or skills required in the role are as follows:	***E/D***
1. Appropriate qualification or significant experience in a relevant discipline, e.g. Information Governance, Data Protection, Information Assurance / Security, MoPI.	E
2. Effective communication skills, dealing with customers and stakeholders at all levels.	E
3. Proven advanced user skills in office computer applications.	E
4. Technical understanding of IT systems and familiarity with Cloud and Mobile technologies.	E
5. Maintain a high degree of integrity and trust when dealing with sensitive and classified information.	E
6. Proven ability to work under pressure, prioritise and manage workload whilst remaining positive and motivated.	E
7. Appropriate professional qualification in relevant discipline, e.g. MSc Information Security, CISSP, CESG Certified Professional etc.	E
8. Appropriate technical qualifications (such as: Security+, CEH, MCSE, CCNA etc.)	E
9. Take actions required to maintain membership of a professional body for the purposes of continuing professional development through shared experience, knowledge and training.	E