Job Title: IT Security Officer	
Job Evaluation Number	B964

JOB DESCRIPTION

Job Title: IT Security Officer	**Location:** Kidlington or Southampton with travel
Job Family: ICT	**Role Profile Title:** BB4 Police Staff
Reports To: Head of Infrastructure	**Band level:** 4U
Staff Responsibilities (direct line management of): IT Security Analysts	

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

The overall purpose of the role is to: Supervise the IT Security function, monitoring technical controls, detecting and responding to IT security incidents in support of the ISO/IEC 27001 Information Security Management System (ISMS). Providing expert Security Architecture 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. Act as a forces' Accreditor and assist the forces' Lead Accreditor through preparing and reviewing risk management documentation and technical risk assessments. Deliver the Information Security strategy across both forces and maintain compliance with national and local information security requirements in support of the ISMS.
2. 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).
3. Responsible for the supervision of the IT Security Analysts including their training and development through the PDR process, motivation, workload planning, welfare, monitoring and quality assurance. Manage staff in support of researching, reviewing, analysing and reporting on IT security issues to produce reports on performance, trends and opportunities to increase IT security.
4. 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.
5. Ensure the Protective Monitoring of technical security controls and respond appropriately to IT security incidents, escalating to the Information Security Manager as appropriate. Identify new and emerging cyber threats and propose mitigations and countermeasures to emerging cyber threats.
6. Responsible for the supervision of the IT Security Analysts including their training and development through the PDR process, motivation, workload planning, welfare, monitoring and quality assurance.
7. 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.
8. Work with the Forces' auditors and act as an accreditor 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).

9. Provide oversight and monitoring of change requests that relate to security enforcing functions to ensure compliance with forces' IT Security policies. Provide oversight and monitoring of Administrative (Sys Admin) access control ensuring that joiners, leavers and movers access is appropriately maintained.
10. Provide expert 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 ICT Security controls and processes.

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

Further Comments:
Advises Technical Architects and Project Managers.
Vetted to the appropriate level to identify and handle sensitive, personal and classified information in accordance with recognised standards and legislation.
Must be able to travel regularly across forces' areas, work equally 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.
Ensure that the IT Security function provides 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. Subject matter expert in IT Security. Hold a degree in Information Security or equivalent qualification (such as: MSc Information Security, CISSP, CESG Certified Professional etc.) or have substantial practical experience in the information security arena.	E
2. Proven ability in providing a high quality of service that meets stakeholder needs whilst remaining within legal and policy frameworks.	E
3. Effective communication skills, dealing with customers and stakeholders at all levels.	E
4. Deep technical understanding of IT systems and appropriate technical qualifications such as Security+, CEH, CCNA, MCSE etc. Must be familiar 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. Take actions required to maintain membership of a professional body for the purposes of continuing professional development through shared experience, knowledge and training.	E