Job Title: Equip Security & Information Assurance Security Analyst	
Job Evaluation Number:	C248

JOB DESCRIPTION

Job Title: Equip Security & Information Assurance Security Analyst	**Location:** Guildford, Lewes or Kidlington
Job Family: Business Support	**Role Profile Title:** BB4 Police Staff
Reports To: Governance and Reporting Lead	**Band level:** 4T
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: be responsible for embedding security assurance best practise across all aspects of the Equip Service. The role holder will be responsible for providing information security assurance for the Equip service by conducting process assurance reviews, as well as risk and impact assessments of all proposed application and infrastructure changes related to Equip. The role will also be responsible for investigating security breaches, conducting audit reviews as well as providing subject matter expertise on Information security to a wide range of Equip stakeholders.

b. **KEY ACCOUNTABILITY AREAS**: Define the important aspects 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. To embed security assurance best practise within Business Systems processes & procedures.
2. Provide information assurance support of SSTVP internal Equip infrastructure And also provide assurance and security oversight for any future integration with the Equip system.
3. Conduct monthly and annual reviews of KPMG security assurance documentation; maintaining records of review and compliance and ensuring any recommendations made in any audit, review or penetration testing of the solution are implemented appropriately.
4. Provide continuous security assurance across all three Force in regards to internal Equip infrastructure; ensuring ongoing compliance with the controls set out in the Security and Information Assurance Matrix for Equip.
5. Conduct assurance reviews of configuration change management for all three Forces for the internal EQUIP infrastructure from an information assurance perspective.
6. Perform associated risk assessments on Equip when any changes occur; ensuring new risks are known and security measures are defined to reduce such risks to acceptable levels.
7. Conduct audit reviews, analysis and reports; ensuring ongoing supplier performance meets the security requirements of all three Forces.
8. Support the investigation of security breaches and other cyber security incidents including documenting such breaches and assessing the damage caused.
9. Provide continuous security assurance of third-party vendors and collaborating with them to meet security requirements.
10. Provide expertise across all areas of protective security, ensuring Equip operates within the relevant legislative frameworks and national guidance and provide advice to the Equip SIRO and Force Accreditors.

11. Produce KPI measures to ensure the IT Security processes are adequately measured and shortcomings are identified.
12. Provide input when required to mitigate or eradicate vulnerabilities within the Equip solution.
13. Ensure patching strategies are applied in a timely manner and understanding the impact on the system when applied.
14. Undertake other duties appropriate to the grade and character of work as may be reasonably required including specific duties of a similar or lesser graded post.

c. **DIMENSIONS**: Include matters such 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:
The job holder will work with internal and external IT support teams and management with the explicit aim of ensuring that all internal force IT Security standards are complied with at all times.
The job holder is expected to use several years' experience in similar roles and knowledge of Force IT security standards to ensure that when violations of policy are discovered either proactively or through reactive reporting, the correct course of action is followed in order to ensure internal and industry standards are maintained.
The job holder is seen as ensuring that Force directives and standards are met. The job holder will have some scope to decide and direct how new standards are implemented and deciding on plans for resolution of non-compliance. Policy decisions will be driven from internal Force IT and industry Security standards.
The role will impact the following parts of the organisation • Internal IT Support teams - ensuring standards are maintained and communicated into and out of Equip. Provide guidance on meeting required standards. • The Forces IT Security teams - ensuring that new standard are understood and implemented and complied with inside Equip. Reporting the Equip compliance position. • External Service Providers – Measuring external supplier security compliance and to ensure non-compliance issues have a plan to address them. Communicating new or changed standards reporting on Equip compliance status, providing security guidance and providing plans to resolve where non-compliance is found.

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 (essential or desirable):	***E/D***
1. An IT security based qualification or equivalent experience, most preferably with ERP.	E
2. Relevant experience and training as an IT security/Information Security Analyst and proven experience in information and security assurance. A good knowledge of current ICT technologies including cloud based, On premise, D365.	E
3. The ability to communicate practical and theoretical knowledge of IT service management to a wide range of stakeholders.	E

4. A good level of understanding of cloud based / SaaS offerings and the Security and Information Assurance associated these type of services.	E
5. A significant level of organisational knowledge to understand the wider impact of security breaches may have on all three Forces and Equip.	E
6. A very good knowledge of networks, operating systems, software, hardware, security and the security risks associated with various infrastructure.	E
7. Strong quality assurance, testing industry knowledge and a strong understanding of patching strategies.	E
8. A very good knowledge of penetration testing, vulnerability scanning and associated techniques as well as an understanding of firewalls, proxies and antivirus concepts.	E
9. The ability to build and manage excellent customer relationships with a diverse range of stakeholders, including third parties in a hosted environment.	E
10. Previous experience of drafting and gaining sign off of procedural documentation as well as planning and progressing their own workloads	E
11. Strong quality assurance and testing industry knowledge.	E
12. A flexible approach to working in an ever changing environment, ensuring role requirements are completed within the deadlines set both independently and in a team.	E
13. The ability to challenge current ways of working and identify new & improved initiatives	E
14. The need to be independently mobile due to the nature of the role and requirement to travel regionally* whilst undertaking all assignments in a timely manner.	
15. Experience of Supportworks and Service Now.	D
Additional comments: The role holder may need to (occasionally) travel to 2nd and third sites to meet with stakeholders. e.g. if the role holder is based in Guildford they may need to (occasionally) travel to Lewes and Kidlington.	