Job Title: Cyber HiTech Investigator	
Job Evaluation Number	B802

JOB DESCRIPTION

Job Title: Cyber HiTech Investigator	**Location:** Near M4 Junction 12
Job Family: Technical Support	**Role Profile Title:** BB3 Police Staff
Reports To: Forensic Supervisor	**Band level:** Entry Level: 3G, Skilled: 3H
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: conduct forensic digital examinations within investigations and operations into the most serious incidents of network based organised criminal activity in order to detect cyber crime; gather and distribute relevant and quality intelligence; to provide technical advice and assistance to officers and staff engaged in the investigation of cyber crime; to produce evidence in a form which is admissible in Court.

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:	***% time***
1. Working to ISO 17025 standards conduct forensic digital examinations of computers, mobile phones and other electronic devices using appropriate processes, methodologies, tools and techniques, in accordance with ACPO guidance and court approved investigative techniques. Identify and secure electronic evidence sources to assist with investigations. Identify and mitigate H&S risks associated with electronic devices. Through these activities provide both an intelligence and evidential product for the SEROCU/Cyber Crime unit.	35%
2. Provide high quality written and oral evidence to support the investigation/operation that can be presented and used by officers/crown prosecution service. Attend Court as a witness in support of such evidence.	20%
3. Assess all immediately available electronic evidence, conduct risk assessments, assess the factors likely to impact on the investigations, check the necessary authorizations, ensure that all material is retained and recorded in order that it can be accessed and used as part of the investigative process. Pass on any relevant information and intelligence to appropriate person(s) and departments, complying with appropriate legislation.	10%
4. Assist in network investigations. This may include, but is not limited to, serious network intrusions which overcome IT systems' architectures and defenses. Investigate the nature, cause and consequences of threats based on the evidence, information and intelligence. Identify victim(s) and potential witnesses in accordance with legislation and policy. This will identify further investigative opportunities within the criminal justice process.	10%
5. Evaluate and report electronic evidence in relation to criminal or civil investigation or to due diligence and maintaining professional standards. Identify further limits of examination as necessary and identify opportunities for further investigation if they exist.	5%
6. With regard to ISO17025 standards and Best Practice Guide to Securing Digital Evidence, capture and preserve electronic evidence carried out at a scene. Conduct any preliminary risk assessments, select appropriate process, tools and preserve the captured data.	5%
7. Maintain current knowledge within field of expertise, keeping up to date with changes through personal development, training and other available resources.	5%

8. Working to ISO 17025 carry out regular checks and validation on equipment held by the Regional Cyber Crime Unit to ensure it remains serviceable.	5%
9. Maintain a help desk facility for the SEROCU on Computer/digital/mobile phones forensics. Deal with telephone enquiries in relation to all technical and administrative issues. Assist in providing statistical information on the unit's performance and achievements.	5%

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:
The role holder will have a high investigative/examination workload in relation to serious and organised crime investigations within the South East Regional Organised Crime Unit. They will be working to strict timescales and deadlines using a number of software packages.
The role holder will carry out forensic digital examinations both in an office and field environment and will be a key member of the investigative team.
The role holder will be technical advisor for cyber crime hardware investigations/examinations within the SEROCU.
The role holder will interact with both internal and external agencies/partners. They will make recommendations to investigating officers/SIO's. They will follow unit SOP and be involved in the initial drafting of these.

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. Good written skills and previous experience of provision of statistical information, with a methodical approach and ability to analyse and produce solutions to problems.	E
2. Ability to work well under pressure, to deadlines and deal with distressing/disturbing material.	E
3. A good communicator – confident and assertive when required - who is able to deal with people at all levels both internally and external agencies, as well as working well in a team.	E
4. A foundation knowledge and experience of a wide range of computer hardware/digital devices (mobile phones)/software/operating systems/networks.	E
5. Willing to make decisions often when working alone and under pressure, taking full responsibility for own actions.	E
6. Able to recognise sensitive information and maintain discretion and confidentiality.	E
7. The post holder must be willing to work flexible hours to suit the requirements of the department and must be willing and able to travel for business purposes, regionally and nationally. Full UK driving licence.	E
8. Previous experience in law enforcement/investigative organisation/s.	D
9. Previous experience of computer/mobile phone forensic techniques/software e.g. Encase, Forensic Tool Kit (FTK), cellebrite, XRY etc.	D

Additional Comments: Post holder should be physically fit with the ability to lift computer equipment and other seized materials, within safe limits including at night. Good eyesight is required with or without corrected vision.

Digital Evidence Investigator (3H) by selection, or to progress to 3H on achievement of all the above, plus the following:	
1. Proven and documented experience in the full role and evidence of managing a significant part of any on-going investigation and how this interlinks with the bigger criminal justice picture.	E
2. Successful completion of the Core Skills in Data Recovery & Analysis/ Core Skills in Mobile Phone Forensics or industry equivalents.	E
3. Vendor-specific foundation level courses e.g. EnCase, AccessData Bootcamp, XRY Foundations etc.	E
4. Professional courses/ certification in SANS, 7Safe, Shrivenham, Control-F, College of Policing courses in Cyber intermediate and advanced.	E
5. Previous experience in computer forensic work AND/OR relevant computing qualification (e.g. MSCE (Microsoft Corporation Certification Engineer) or HNC in Computing) plus knowledge of the internet and networking.	D

Problem Solving: All role holders are confronted regularly with problems, they are presented with new or unusual situations, demands or challenges, or something has gone wrong and has to be sorted out.

The problems that have to be dealt with in carrying out this role include:
1. Managing the needs/expectations of customers and external partners/agencies who have limited technical/computing forensic knowledge. Providing detailed explanations that can be understood and used to direct an investigation.
2. Managing and understanding new and emerging technical issues related to cyber crime, cyber enabled crime and utilising these techniques in the investigations/operations of the unit.

Planning: Refers to any problems that may be met in planning because of the unpredictability of the workload or the time scales over which plans have to be made.

The role involves the following planning activities:
1. Planning and prioritising workload, ensuring high standards are maintained when working under pressure.
2. Short notice change to planned work, unplanned change in operational requirements, due to the nature and scope of SEROCU investigations/operations.

Freedom to Act: Describes the scope the role provides to act independently without seeking prior approval from the manager or colleagues.

The degree to which the role provides freedom to act is as follows:
1. Identifying and utilising best practice forensic digital techniques/software during an examination.
2. Advising investigators/senior officers/staff, on forensic matters and available for digital forensic examinations that are applicable and how they can be used appropriately during each investigation/operation.
3. Offering specialist advice during search warrants, suspect interviews, investigations, case conferences and court.

Interpersonal skills: Describes the ways in which the job relates to people and uses interpersonal skills.

The role involves exercising interpersonal skills as follows:
1. Role holder will work as part of a small specialist unit within a larger regional unit. They will be expected to work ethically and act in a professional manner with all other members of staff.
2. There will be an expectation that they will be able to liaise with external law enforcement agencies, partner organisations and industry bodies.
3. Ability to act as point of contact for the Cyber Unit when representing the unit on operations/investigations, locally in forces, regionally and nationally.

Communicating: Indicates what sort of communications are made in carrying out the role, the format (oral or written), the purpose and frequency and to whom they are addressed.

The role involves communicating to people as follows:
1. Communicating ideas and understanding effectively, both verbally and in writing. Using language and style of communication that is appropriate to the situation and people being addressed. This includes communicating highly technical matters/information to a wide audience.
2. Communication with other staff within the cyber crime unit and SEROCU, including other regional and national units and outside agencies/industry.
3 Presenting evidence at court in a written/diagrammatic way, but also attending court in person and giving evidence with the criminal justice process