



south east

Regional Organised Crime Unit

CONSTABLE ROLE SPECIFICATION

Role Title:	Detective Constable Cyber Crime	Department:	Cyber Crime - Pursue
Reports To:	Detective Sergeant - Cyber Crime	Location:	South East Regional Organised Crime Unit (SEROCU)

Purpose of role:	To conduct investigations and operations into the most serious incidents of network based organised criminal activity; to detect digital crime; gather and distribute relevant and quality intelligence; to provide technical advice and assistance to officers engaged in the investigation of digital crime; to produce evidence in a form which is admissible in Court. This is carried out in relation to cybercrime as defined by the Home Office and the National Strategy.
Principle Responsibilities:	Identify and secure electronic evidence sources to assist with investigations. Check that necessary authorizations are in place, conduct preparatory research including open & closed source concerning the capabilities of the individual subject of the investigations and/or the functionality of the relevant digital evidence sources to which they give access. Identify H&S risks associated with the electronic devices.
	Working to ISO17025 & ISO17020 standards, seize and record electronic evidence sources. Take appropriate safeguards, photograph and label the components of the device, appropriately package, seal and label the device in accordance with ISO17025 SEROCU Procedural Guidelines.
	Working to ISO17025 & ISO17020 standards, capture and preserve electronic evidence carried out in a laboratory. Conduct any preliminary risk assessments, select appropriate process, tools and preserve the captured data in line with the ISO10725 SEROCU Procedural Guidelines.
	With regard to ISO17025 & ISO17020 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. Support the SEROCU Digital Forensic Unit by deploying as required to provide technical support for a range of digital devices including server capture or network investigation.
	To work to ISO17025 & ISO17020 SEROCU Procedural Guidelines to ensure that Cyber PURSUE & Digital Forensic Units achieve and

	maintain ISO17025 & ISO17020 accreditation. To ensure that Training and Competency is maintained and appropriately recorded.
	Investigate electronic evidence in relation to criminal investigation, or to due diligence and maintaining professional standards. Conduct investigation using appropriate processes, methodologies, tools and techniques.
	Evaluate and report electronic evidence in relation to criminal investigation or to due diligence and maintaining professional standards. Identify further lines of examination as necessary and identify opportunities for further investigation if they exist.
	Conduct Open Source Internet investigations. 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. Pass on any relevant information and intelligence that may be relevant to appropriate person(s) and departments. Comply with appropriate legislation.
	Conduct network investigations. This may include, but is not limited to, serious network intrusions which overcome IT systems' architectures and defences. Investigate the nature, cause and consequences of a threat based on the evidence, information and intelligence. Identify victim(s) and potential witnesses in accordance with legislation and policy.
	Recover technical equipment. Prepare and plan to recover technical equipment, disconnect, dismantle and return technical equipment.
Essential role based training:	Substantive PIP 2 Detective Constable
Essential Criteria:	<ul style="list-style-type: none"> • Ability to evidence computer qualifications including computer forensic qualifications (Essential) or Evidenced previous employment within computer or IT industry (Essential) • Experience of working with computer systems e.g. servers (Essential) • Proven ability to handle intelligence/sensitive information (Essential) • Ability to work effectively within a team as well as independently and to operate under pressure (Essential) • Effective communication and interpersonal skills (Essential) • Has completed a CID foundation course or successfully completed the ICIDP (Essential)
Desirable Criteria:	<ul style="list-style-type: none"> • Experience working in the cyber and digital environment and knowledge of the practical challenges this presents. (Desirable) • Substantive Detective Constable (Desirable)
Competency Value Framework (CVF) - Level 1	<ul style="list-style-type: none"> • We are emotionally aware • We take ownership • We collaborate • We deliver support and inspire • We analyst critically • We are innovative and open-minded

