

## Digital Forensic Unit Senior Technical Specialist

---

**Department:** Justice and Home Affairs

**Division:** States of Jersey Police

**Reports to:** Head of Digital Forensics Unit

**JE Ref:** JHA1121

**Grade:** CS12

**JE Date:** 06/03/2023

### Job purpose

The Digital Forensics Unit (DFU) is an integral centralised department within States of Jersey Police (SoJP) for the recovery, production and interpretation of digital evidence. It is the fastest emerging growth area of policing and with rapidly changing technological advances it impacts all of today's aspects of policing.

The post is a leading technical role, responsibility for ensuring that the States of Jersey Police has the technical competency and capabilities to respond to all current and emerging forensic challenges, ensuring the DFU remains at the forefront of forensic analysis.

To act as a subject matter expert across all the digital forensic disciplines, conducting and managing highly complex investigations, presenting findings and providing advice and guidance to stakeholders at all levels. Present and explain impartial technical expert evidence within courts of law in Jersey and abroad, assisting the judiciary in making informed decisions in all types of criminal and civil cases.

The Digital Forensic Specialist reports into this Senior Technical Specialist role.

### Job Specific Outcomes

- 1 Responsible for the technical leadership of the Digital Forensic Unit, working alongside and deputising when required for the Head of Digital Forensics Unit. Providing the technical input and guidance required when setting and agreeing high level strategic priorities, developing service level agreements, determining case priorities and submission screening.
- 2 Overseeing the provision of technical investigative services and advice to the SoJP, other States departments (e.g. Customs and Immigration), commercial organisations and international Law enforcement agencies.
- 3 Responsible for the performance management of the DFUs operations and the monitoring and reporting of KPIs to the Head of Digital Forensics Unit through the use of metrics. Identifying trends, forecasts and areas of risk to enable evidence based strategic decisions.
- 4 Control the strategic design, management and security of the departments network infrastructure and high risk interconnects with external systems.

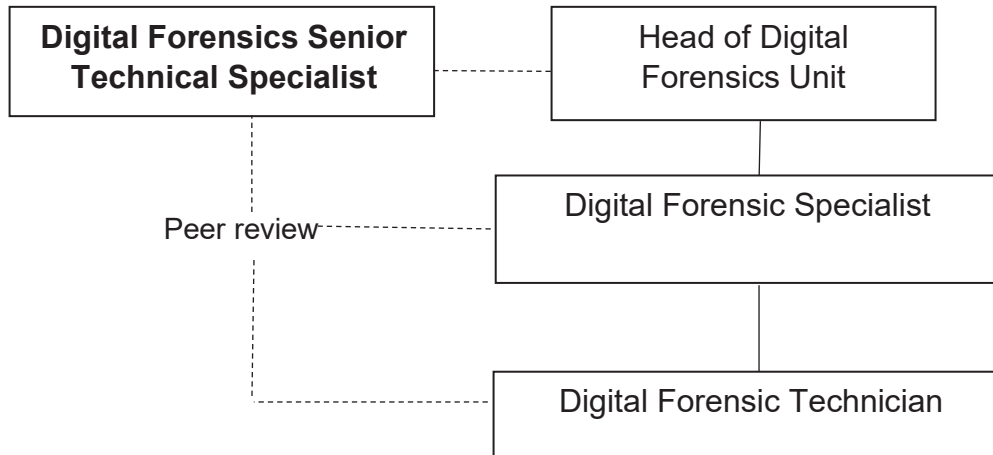
- 5 Provide day-to-day technical oversight of the department and assisting and advising with case work and professional development of the staff. Perform technical peer reviews, including the re-examination of devices, reviewing forensic output and ensuring compliance with relevant standards.
- 6 Overseeing the preparation and dissemination of best practice guidance, policies and procedures relating to the handling and forensic examination of digital evidence.
- 7 Manage and prioritise investigations based on urgency and risk, maintaining continual communication with all stakeholders to manage expectations.
- 8 Ensure Jersey maintains its ability to solve complex crimes involving digital devices, through research and development, training, knowledge sharing and establishing and maintaining technical links and trusting relationships with leading subject matter experts, overseas agencies and international forensic networks.
- 9 Develop and maintain the department's technical capabilities and support the wider forensic community through the creation of new and innovative forensic software tools and continued development and maintenance of existing in-house software systems and databases.
- 10 Oversee the management of the complete DFU infrastructure, which includes the forensic systems, software and network fabric, ensuring all areas remain efficient, effective and compliant with legal requirements. Identify areas to restructure or improve, producing relevant business cases as required.
- 11 Carry out comprehensive forensic examinations of any digital device or computer network forming part of a criminal investigation, working and co-ordinating across all SOJP departments, other States departments (e.g. Customs and Immigration) together with Law enforcement agencies based outside Jersey.
- 12 Lead and coordinate large and complex forensic or cybercrime investigations, involving multiple investigators and technical specialists. Managing all technical aspects of the investigation, from capture to courtroom.
- 13 Prepare and present a wide variety of different material, including business cases, departmental metrics and technical evidence in the form of reports, witness statements and oral testimony to a wide range of audiences, including senior and executive staff, case officers, partner agencies, overseas law enforcement agencies, Industry, legal advisers and members of the judiciary.
- 14 Attend court at both home and abroad, to present and explain complex technical evidence in a form which can be readily understood and evaluated. Stand as an Expert Witness, providing personal opinion and advising the Court on all relevant technical aspects of the case.

### **Statutory responsibilities**

Active engagement, participation and compliance with any other statutory responsibilities applicable to the role, as amended from time to time. This role has specific legal obligations

in terms of providing evidence on oath for every criminal investigation. The officer is required to provide sworn witness statements.

### Organisation chart



## Person Specification

### Specific to the role

ATTRIBUTES	ESSENTIAL	DESIRABLE
<b>Qualifications</b>	<p>A degree or equivalent.</p> <p>Required to be educated to RQF Level 7, holding a master's degree, PGCert or equivalent in a forensic computing or cyber security related subject.</p> <p>Formal certified training in multiple forensic products to an advanced level.</p> <p>Industry recognised professional qualifications such as CCNA-Sec, CISSP, CITP.</p> <p>Full membership of a relevant professional body, such as the British Computer Society or Chartered Institute of Information Security.</p>	
<b>Knowledge</b>	<p>Background in Digital Forensics or cyber security with experience working across multiple different specialisms and disciplines, including computer forensics, mobile forensics and cyber security investigations.</p> <p>Demonstrable deep technical knowledge and</p>	

	<p>specialism in computer forensics, mobile forensics or network forensics with sufficient experience and the broad knowledge to perform forensic examinations across any of the different digital forensic disciplines.</p> <p>Extensive and demonstrable knowledge of network environments, cyber security threat vectors and network forensics. Ability to manage and undertake complex cybercrime investigations within a broad range of possible scenarios. Experience and skills to respond appropriately to active threat actors to secure evidence and protect infrastructure.</p> <p>Demonstrable knowledge of one or more programming languages to support and further the development of in-house forensic systems and to enable the rapid development of innovative solutions to complex problems.</p>	
<p><b>Technical / Work-based Skills</b></p>	<p>Exemplary problem-solving and analytical skills with a structured and logical approach which can be applied to a diverse range of scenarios. The ability to identify, link and assimilate evidence from a wide variety of digital and non-digital data sources.</p> <p>The technical expertise to perform in-depth complex forensic examinations of devices together with the technical competency to undertake work in other IT related areas as required.</p> <p>A diverse technical background with the expertise to work across different technical domains. Utilising knowledge from different technical fields to establish a sequence of events and support or dispute a theory, frequently requiring creative thinking and a flexible mindset to develop novel methodologies, define new approaches or create custom programmes/tools to solve particular problems.</p> <p>Ability to make their own interpretation of the laws applicable to the offence being investigated, with respect to computer based evidence, taking into account legal precedents and case law.</p>	
<p><b>General Skills/Attributes</b></p>	<p>Excellent communication and written language</p>	

	<p>skills, with the ability to communicate highly technical information to a wide range of audiences Ability to influence and build consensus at all levels.</p> <p>Excellent planning and organisational skills to manage an unpredictable and varied workload efficiently, reacting rapidly to changing priorities within a high-pressure environment. Ability to operate with a high degree of autonomy without supervision, independently making crucial decisions with accountability.</p> <p>The interpersonal and intellectual ability to build effective and trusting relationships with the DFU's diverse range of stakeholders and to act as an effective mentor to less experienced members of staff.</p> <p>Confidence and credibility to present Expert testimony in courts, both within Jersey and abroad, on complex, sensitive and technical cases. The ability to defend, reason and justify effectively whilst under cross examination from defence teams and other technical experts.</p> <p>Ability to work and liaise with other law enforcement agencies around the world on joint investigations, intelligence sharing and the sharing of new investigative tools and methodologies.</p> <p>Accomplished technical leader and teambuilder who can create a culture of outstanding performance that promotes information and skills sharing and engenders trust.</p> <p>Full Driving License</p>	
<p><b>Experience</b></p>	<p>Significant experience in a similar role operating within a cyber-response or digital investigation team at a senior level.</p> <p>A minimum of five years' experience performing forensic or cybercrime investigations within multi-disciplined environments.</p> <p>Experience managing operational teams and leading large investigations spanning multiple technical disciplines.</p>	

	<p>Experience of policy and process design and implementation. Proven experience leading, coaching and mentoring a technical team to deliver world-class services.</p> <p>The post holder must have relevant Court experience or be able to demonstrate their ability to deliver evidence as an Expert Witness.</p>	
<p><b>Criteria relating to Safeguarding</b></p>	<p>Exposure to unsavoury, confidential and sensitive issues where the careful and effective handling of such matters is essential.</p> <p>Maturity and stability to cope with assessing distressing picture and movie files of a sexual, violent and degrading nature, often involving children. Due to the nature of material encountered, there is a requirement to attend scheduled welfare checks.</p> <p>Requirement for high levels of integrity, tact, resilience and discretion, which are essential when dealing with sensitive intelligence and other information.</p>	

### Core Accountabilities, Attributes and Behaviour Indicators

Appointees to this role will be required to adhere to and perform their duties in line with the standards identified in the States of Jersey tier 1-3 core accountabilities attributes and behaviour indicators.