Specific Role Profile

This Specific Role Profile sheet covers specific areas of activities that are not included in the Generic Role Profile. It will include responsibilities, knowledge, skills, delivery and working arrangements relevant to this role. Please ensure that this is read and in conjunction with the given family role for the post.

Profile Owner: Head of WMCTU

POLICE STAFF

ROLE SPECIFIC INFORMATION	
Job Title:	Head of IT and Security
Generic Role Profile:	Information Technology and Security
Salary Grade:	12
Operational / Non Operational Role	Non-Operational
Vetting Level:	Developed Vetting
Reporting to:	Head of WMCTU
Responsible for:	Line management of ICT Support, Information Security, Physical Security, National Security Vetting department, OPSY and STRAPSO functions.
Specific Role Purpose:	As a key member of the Strategic Leadership Team, the post holder will be responsible for the leadership of a multi-disciplined department incorporating Information Technology, Informational Security, National Security Vetting, OPSY and STRAPSO functions, physical security of all CTPWM infrastructure including Regional Special Branches as well as the personal security of all CTU personnel and visitors at any CTPWM Estate. The post holder will act as a trusted advisor to the Head of CTPWM, wider Command Team and key partners on all matters relating to technology and security, ensuring all issues are understood and appropriately managed. With an IT budget alone of close to £3 million, this is a broad and varied portfolio which allows the post holder the ability to set strategy and direction and engage key stakeholders across policing, the wider CT Network and external partners. This role has a high degree of independence and is responsible for the provision of specialist services across the whole of the organisation, requiring decisive direction.
Specific Role Responsibilities:	**Overarching** • Develop and execute an IT and Security strategy ensuring it is effectively aligned with the vision and objectives of the wider counter terrorism unit, host force as well as National CT headquarters. • Act as a strategic advisor to the Head of CTU, wider command team and partners on strategic matters within the portfolio, recommending solutions to both existing and forecasted strategic risks or problems.

- Develop and enforce policies, procedures and standards to protect the organisations data, systems, personnel and infrastructure against internal and external threats.

- Lead on IT and Security change and transformation projects and programmes, collaborating with key stakeholders to successfully deliver technology and non-technology led change.

- Work closely with key internal and external stakeholders, ensuring compliance with legal and regulatory laws and standards.

- Develop and maintain appropriate governance that supports the needs of the organisation.

- Oversee CTPWM accreditation processes, including penetration testing for physical site security, IT systems and Information Security purposes, ensuring compliance with the relevant industry and security regulations and standards.

- Provide reassurance to the Head of Unit and key external partners that all systems, procedures and policies are compliant.

- Act as the senior representative for the unit with regards to information technology and security at local, regional and national governance, developing and maintaining collaborative strategic relationships.

- Responsible for the departments Risk Management framework which seeks to identify, assess, manage and mitigate risks around Information, Personnel, Technological and Physical infrastructure.

- Lead, motivate, engage and develop a team of professionals and provide leadership to a significant area of responsibility, protecting and promoting workforce wellbeing and professional standards.

- Lead the assessment of future demands and emerging threats within IT and Security, developing and adapting plans to ensure that these demands/threats are effectively anticipated and met.

Security

- Accountable for all aspects of physical security to ensure the provision of a safe and secure environment for all staff and visitors across the WMCTP estate.

- Responsible for the National Security Vetting of all relevant WMP/CT personnel as well the vetting of all national contractors, to safeguard national security and help maintain public trust and confidence.

- Responsible for the development and implementation of a local security

regime including regular walkthroughs and audits to identify, assess and mitigate any risks or vulnerabilities.

- Accountable for the development, implementation and monitoring of an Information Security Strategy ensuring continued accessibility, integrity and confidentiality of our information on behalf CTPWM and partners.

- Accountable for developing a strong 'security' culture for the entire region, providing regular security education and awareness.

- Commissioning and co-ordinating work within the appropriate business areas to eliminate, reduce or mitigate against any threats or risks identified.

IT

- Control and management of the annual £3 million revenue and capital budgets for IT, developing business case justifications and cost/benefit analyses for spending and initiatives as well as future forecasting.

- Lead on IT strategic procurement, managing all third-party liaison and maximising value for money. Includes contract renegotiations, supplier performance monitoring, risk mitigation and ensuring agreed standards and targets are met.

- Set the strategy for monitoring and managing the performance of IT-related systems and services, in respect of their contribution to business performance and benefits to the business.

- Responsible for the development, security, capability, availability, and performance of all CTPWM IT systems including the physical and virtual infrastructure.

- Develop and manage an incident response plan and associated recovery plan, ensuring organisational preparedness and resilience against IT security incidents.

- Development of strategy and aligned culture to support transformation and innovation, promoting the opportunities that technology presents, including the feasibility of change and its likely impact upon the business.

- Identify opportunities for the appropriate and cost-effective investment of finance in IT systems and resources, including sourcing, purchasing, and in-house development.

SPECIFIC COMPETENCIES REQUIRED FOR EFFECTIVE PERFORMANCE	
Knowledge & Experience *This section should detail the requirement of previous experiences and knowledge gained from academic qualifications if appropriate, e.g. significant experience of administrative duties, degree level educated.*	
Essential:	Post holders will be required to display and evidence: • Educated to degree level or have a minimum of 5 years experience in a relevant field. • Extensive leadership experience in leading a multi skilled team. • Experience of negotiating effectively with a wide range of executives both internally and externally. • Experience of working closely with senior executives to develop organisational strategy. • Proven track record in managing and coordinating complex ICT transformation projects. • Proven experience in developing and implementing IT and security strategies and plans. • Evidence of proactive business change management and delivery of service with a good understanding of existing and emerging technology together with the ability to identify the wider implications and interdependencies of any change. • Delivery of innovative solutions that support improvement initiatives to achieve organisational excellence and support the business plan. • Experience in Information Security, creation and compliance to policies and standards. • Excellent communication skills, with the ability to explain complex security and technology-based matters. • Financial experience and budget management.
Skills *This section should detail the competency requirement which could be developed through non formal training e.g. effective time management, influencing and negotiating, effective communication including written and verbal.* *Refer to skills database for core operational skills*	
Essential	• A good knowledge of IT Infrastructure, current IT Industry trends and Communication technologies. • A good knowledge of provision of security, including physical, personnel, assets, information handling and communications. • Customer focus and an ability to develop key stakeholder relationships to enhance operational performance and develop the business. • Skilled in planning and objective setting to medium and long-term cycles, coordinating a complex range of activities. • Able to make operational and business decisions, applying appropriate frameworks, models and risk management processes and anticipating the implications of decisions. • Able to use a range of communication and influencing techniques and methods to successfully negotiate, collaborate and/or effect change.

Desirable:	• An awareness of ITIL
Hours of Work and Flexibility:	The post holder will be contracted to work 36.5 hours per week but will need to be flexible to meet the demands of the post, and may have to work outside normal core hours. They will need to have the ability to travel to different locations as required.
Restriction Level:	