**ROLE PROFILE**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Role Title:** | | Endpoint Management Engineer | **Leadership level:** | *To be determined at later phase* | |
| **Post reference:** | | 20125 | **Job family:** | *To be determined at later phase* | |
| **Grade:** | | F/G/H tbc | **Location:** | Ponteland (NWOW – Flexible Worker) | |
| **Allowances:** | | Casual Car Allowance | **Politically restricted post:** | NA | |
| **Area command / Department:** | | Digital Policing,  End User Services | **Vetting level:** | RV - access to official sensitive and occasional secret information | |
| **Reporting to:** | | Senior Endpoint Management Engineer | **Date accepted as a role profile:** |  | |
| **Posts responsible for:** | | NA | | | |
| **Part A – Job Description** | | | | | |
| **Overall purpose of the role:** | | | | | |
| Participate in the delivery of a performant, cost effective and appropriately resilient endpoint management service, that meets the agreed service level for critical business functions.   * Provide primary delivery of the end user device desktop and mobile client platforms. * Perform application repackaging and deployments in order to integrate systems seamlessly into production. * Apply security patching of the client operating systems and business applications. | | | | | |
| **Key responsibilities of the role:** | | | | | |
| **1** | Participate in the effective delivery and subsequent 2nd line support of the ICT endpoint management services including   * desktop troubleshooting, * device configuration, and * device management systems utilised by ICT support teams. | | | | |
| **2** | Participate in the effective delivery of an Incident and Problem Management service identifying potential problems and trends within endpoint management environments, assessing whether the performance of the systems is aligned to agreed Service Level Agreements. | | | | |
| **3** | Deliver secure, robust, zero touch application deployment packages, and engage with stakeholders to plan deployment delivery options. | | | | |
| **4** | Desktop build management – the ongoing creation, configuration and testing of new builds/operating system deployments/Windows versions to maintain operating system compliance and leverage the latest features. | | | | |
| **5** | Desktop/laptop and server operating system security patch management – Monitor and progress the delivery of updates to ensure devices are securely patched within agreed timescales. Identify problem devices and take or recommend mitigating action. | | | | |
| **6** | Active Directory administration of users, computers and groups in relation to desktop configuration, deployment, and security.  Group policy administration and application as required to support device delivery, configuration, standardisation and security at an enterprise level adhering to current design. | | | | |
| **7** | Undertake auditing of hardware and software inventory, verify results, and produce reports collated from several data sources. | | | | |
| **8** | Maintain and configure VMWare Virtual Desktop Infrastructure client devices, including application content and security updates. | | | | |
| **9** | Liaise with internal and external user groups, manufacturers and suppliers as required in order to maintain force capabilities and to provide technical input and support the needs of the business. | | | | |
| **10** | Liaise with key ICT stakeholders to ensure the provision of a fully integrated efficient, effective, and customer focused, Endpoint Management service. | | | | |
| **11** | Participate in the compliance with Information Security requirements, maintaining appropriate documentation. | | | | |
| **12** | Manage enterprise level deployments and configuration changes, with an understanding of the complexities and risks present in large scale implementations. Fully understand the department change control process, and how this is an integral part of any large-scale deployment. | | | | |
| **13** | Use enterprise level device management systems at full administrator level, with responsibility for securing and maintaining user and device access to those systems. Using queries and experience, create automated user and device collections and groups to best maintain an optimum environment for deployment and device management. | | | | |
| **14** | Carry out testing of any system element (e.g. installation, script or device) before introduction into production environment, ensuring design and security standards are met and adhered to, and any issues are formally communicated to all stakeholders. | | | | |
| **15** | Administer End User devices managed by appropriate MDM (mobile device management) solutions, ensuring configuration, security and deployments adhere to architectural design specifications. | | | | |
|  | | | | |
| **Part B – Scope of contacts** | | | | | |
| **Internal / External relationships:** | | | | | |
| **Internal:** System Owners and DP service users, DP Team Leaders, Technical “Gatekeepers” across the force including within DFU/TSU/NERSOU  **External:** Suppliers, colleagues from other forces, local authorities | | | | | |

|  |
| --- |
| **Part C – Competencies and Values** |
| **Northumbria competencies and values framework (NCVF)** |
| *Level – tbc*   * The Endpoint Management Engineer role is a career graded role. The expectation is that staff will be appointed into the role at F grade and can proceed to the top of grade G by performing well in the role. A career development matrix is maintained for this role that identifies the skills and experience that must be demonstrated by the post holder prior to them progressing onto grade H. * To progress to Grade H the post holder will create a portfolio of evidence in their PDR and they will present this evidence to their line management team. If they can demonstrate that they are ready to progress their line manager will confirm this to People Services. |

|  |  |
| --- | --- |
| **Part D – Continuous Professional Development (CPD) role 6 months** *To be determined* | |
| **First 6 months** | |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| **12 months and beyond** | |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |

**Part E - PERSON SPECIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Essential** | **Desirable** | **How to be assessed** |
| Qualifications, knowledge and experience | In-depth experience of Microsoft Endpoint Management Configuration Manager (SCCM).  Knowledge of application packaging for deployment, using scripts where appropriate.  Windows 10 administration and configuration experience.  An understanding of the need for patch management, and product lifecycles.  Experience of using an ITSM tool | Experienced in the use of Microsoft cloud services (Intune, Endpoint Manager Admin, Azure, Autopilot, M365) at Intune administrator level.  Microsoft MD101: Managing Modern Desktops  Microsoft MD100: Windows 10  Mobile Device Management with Intune/Endpoint Manager.  Group policy administration.  Experience of managing enterprise deployment solutions.  Powershell scripting experience.  Experience of T-SQL, WQL, CMPivot, and Kusto for Intune analytics.  An understanding of Windows Installer technologies. | Application/interview/  CPD |
| Planning and organising | Ability to manage and prioritise own workload, and work effectively to deadlines in a fast-paced changing environment.  Identify potential problems and trends on endpoints by ensuring that the performance of the systems and support services remain in line with the SLA’s to provide an outstanding customer focused service.  Understanding of the reasons for planned testing, log analysing, and approval before changes are implemented in the production environment. | To undertake sub-projects which will involve research and connecting with internal and external parties. | Application/interview/  CPD |
| Problem solving and initiative | Demonstrate advanced troubleshooting skills with regard to operating systems and configuration management tools.  Within demand, design and security constraints, it is expected the role holder will be able to work independently and under own initiative. | Demonstrate the ability to spot trends and potential problems, then recommending mitigating actions.  Research and develop new technology, tools and scripts to support the delivery of desktop computing and improve the end user device experience. | Application/interview/  CPD |
| Management and teamwork |  | Ability to take ownership/share tasks between colleagues to achieve required results | Application/interview/  CPD |
| Communicating and influencing | Excellent verbal and written communication skills to effectively collaborate and connect with both business and technical IT teams.  Your experience of large-scale deployments and/or technical knowledge will influence project decisions relating to new services or changes. | The ability to empathise and understand problems from a customer perspective and use that insight to manage a satisfactory resolution. | Application/interview/  CPD |
| Other skills and behaviours | Focusing on and adapting to the customer’s needs to deliver satisfaction to the wider business. | A keen learner with a genuine interest in endpoint management.  Experience of working in a public sector or police force environment | Application/interview/  CPD |