****JOB DESCRIPTION

|  |  |  |  |
| --- | --- | --- | --- |
| Job Title | **(Trainee) ICT Security Engineer** | Post Number | **F1058** |
| Career Grade | 6 – 9  Trainee at Grade 6 | Service Area | ICT |
| Special Conditions | Ability to travel to various locations in response to ‘call outs’ at short notice.  Availability to work occasional weekends/evenings. | Additional Benefits | Casual car user |
| Authorised by | Deputy Chief executive | Date | June 2024 |

**Job Purpose**

|  |  |
| --- | --- |
| The purpose of this role within the Council is: | To be member of team with responsibility for the security of all South Worcestershire ICT shared service systems |
| Responsible for demonstrating commitment to working in line with the Councils' values | |
| Responsible for championing and demonstrating the Council’s Leadership Behaviour Framework | |
| The postholder works for: | Cyber Security Manager |
| The postholder manages \supervises: | None |

|  |  |
| --- | --- |
| **This post is career graded. Indicative levels of responsibility at each grade are as follows** | |
| Grade 6 | Trainee – Assist with vulnerability scanning; software patching; monitoring of ICT security systems |
| Grade 7 | Responsible for Vulnerability Scanning; Software Patching; and Supported Application Compliance. Other technical duties with support from Cyber Security Manager. |
| Grade 8 | Independently responsible for all technical duties below but with support from the Cyber Security Manager for Investigations; Application Security; Infrastructure Security; and Web Security. |
| Grade 9 | Independently responsible for all duties below. |

|  |  |
| --- | --- |
| **Key Accountabilities (All accountabilities will be carried out in line with the Council’s policies, procedures and relevant regulations and legislation)** | |
| 1 | Vulnerability scanning:   * + Perform regular vulnerability scans of all ICT systems and devices.   + Produce work plans providing details of all critical and high vulnerabilities that need to be addressed. Ensuring that vulnerabilities are addressed within prescribed timescales. |
| 2 | Software Patching:   * + Working with infrastructure and application teams ensure that automated patch management tools are working so that patches for critical and high vulnerabilities are applied within 14 days of identification. |
| 3 | PSN Compliance:   * + Organise annual ICT health check.   + Produce action plan to address any vulnerabilities identified by ICT health check.   + Ensure completion of PSN submissions |
| 4 | PCI Compliance:   * + Review reports from PCI compliance organisation (currently Securitymetrics)   + Act on reports and ensure any vulnerabilities are addressed within prescribed timescales.   + Maintain awareness of requirements for PCI compliance and ensure that any measures are implemented. |
| 5 | Cyber Essentials   * + Ensure Cyber Essentials accreditation is maintained.   + Review responses required to meet accreditation.   + Ensure any actions required are implemented to maintain accreditation. |
| 6 | Investigations:   * + Confidentially carry out investigations and produce reports on:     - Internet usage     - Email usage     - Account activity     - Any other ICT related investigation |
| 7 | Monitoring SIEM (Security Information and Event Management)   * + Manage SIEM systems in place to ensure they provide proactive reports of security breaches.   + Act immediately on reports to ensure breach resolved effectively and swiftly. |
| 8 | Monitoring of security information from external sources   * + Monitor sources of security information and ensure information appropriate for South Worcestershire ICT is acted on in appropriate timescales. Sources of information include:     - CERT-UK     - NCSC     - US-CERT |
| 9 | Supported application compliance:   * + Maintain list of all applications and other software in use including maintenance support and end of life (unsupported) dates if appropriate.   + Work with other members of ICT and Service Users on transition plans to ensure on supported applications are run on South Worcestershire ICT systems. |
| 10 | Application Security:   * + Maintain awareness of areas of vulnerability in security of software applications.   + Work with business application team to ensure all applications in use meet appropriate security levels. |
| 11 | Infrastructure Security:   * + Maintain awareness of areas of vulnerability in security of ICT infrastructure.   + Work with infrastructure team to ensure all infrastructure in use meets appropriate security levels. |
| 12 | Web Security:   * + Maintain awareness of areas of vulnerability in security of web based applications.   + Work with web and self-service team to ensure all web and self-service applications in use meets appropriate security levels. |
| 13 | Incident Response:   * + Ensure that appropriate incident response procedure is in place to handle critical ICT security incidents.   + Ensure that all ICT staff are aware of the procedure and have been trained in its implementation.   + Carry out six monthly exercises to ensure procedure can handle current threats effectively. |
| 14 | Reporting:   * + Produce regular reports on ICT security including:     - Number and type of security incidents     - Effectiveness of ICT security measures in place     - Recommendations on improvements to ICT Security     - Business cases to support improvement recommendations if requested.   + Report security incidents to external bodies including police and National Cyber Security Centre. |
| 15 | Research and Advice   * + Carry out regular research into current ICT security threats and measures to mitigate risks. |
| 16 | Policy   * + As required develop or amend ICT security policy for South Worcestershire ICT systems |
| 17 | Data Protection   * + Work with South Worcestershire DPO’s (Data Protection Officers) on any issues arising with regards to Data Protection and in particular the GDPR. |
| 18 | To be aware of your responsibilities in terms of health and safety, including identifying at your appraisal, appropriate health and safety training. |
| 19 | Customer Focus;   1. Provide technical consultancy to the service units on any ICT security issues and developments as required. 2. Ensure you approach your duties taking into consideration the principles of value for money and a flexible, customer focused approach. |
| 20 | Corporate Contribution;   1. Have a good working knowledge of the priorities of central government in the areas of planning, place shaping, digital by default, government and industry standard, Freedom of Information (FOI) Act 2000, Data Protection 1998, Computer Misuse Act 1998 and key deliverables outlined in ICT strategy. 2. Provide accurate and timely reporting, documentation and updates to the business as required. |
| 21 | General Duties;   1. To undertake such other duties, training and/or hours of work as may be reasonably required and which are consistent with the general level of responsibility of this job. 2. Any other duties that may be required from time to time, depending on the exigencies of the service. 3. In all contacts the postholder will be required to present a good image of South Worcestershire ICT shared service Directorate and the Council as well as maintaining constructive relationships.   Internal: All ICT Shared Service partners and staff  External: Suppliers, external agencies and other Council officers. |

**NOTES:**

1. Duties will inevitably develop and change as the work of the Council changes to meet the needs of our customers. Employees should therefore expect periodic variations to job descriptions, and the Council retain this right. This job description will be supplemented on a regular basis by individual objectives derived from Council strategies.
2. Where an applicant or an existing employee is or becomes disabled (as defined by law) and inform the Council fully of their requirements reasonable adjustments will be made to the job description wherever possible.

KEY REQUIREMENTS

CAREER GRADED POSTS

Appointment to and progression through career grades is dependent upon:

* Achieving the relevant qualifications and experience detailed in the Key Requirements
* Line Managers confirmation of satisfactory performance in the post and recommendation for progression
* Line Manager confirmation that postholder is required to undertake the level of responsibility required at the next grade
* Postholder’s ability to undertake such work.

Normal incremental progression within the grade will apply until the postholder meets the above criteria for progression to the next salary grade.

|  |  |  |
| --- | --- | --- |
| Qualifications (or knowledge and experience at an equivalent level) | Essential for grade | Desirable |
| Degree or equivalent qualification and/or practical experience working in an ICT environment | 6, 7, 8, 9 |  |
| Working towards CISSP qualification. | 9 |  |
| ITIL Foundation |  | All grades |

|  |  |  |
| --- | --- | --- |
| Experience | Essential for grade | Desirable |
| Ability to work on assigned security tasks under supervision | 6 |  |
| Ability to work on assigned security tasks and ICT projects under supervision | 7 |  |
| At least one years practical work experience of ICT security involving vulnerability scanning, investigations, compliance and reporting. | 8 |  |
| Able to work independently on ICT security tasks assigned by manager. | 8 |  |
| At least three years practical experience of ICT security involving vulnerability scanning, investigations, compliance and reporting. | 9 |  |
| Experience of advising at a corporate level on ICT security . | 9 |  |
| Able to identify and work independently on ICT security tasks and projects. | 9 |  |
| Experience of working through change in a complex organization. |  | All grades |
| Knowledge of ICT issues at a national and local level, including national Digital by Default Strategy and place shaping. |  | All grades |

|  |  |  |
| --- | --- | --- |
| Skills Required | Essential for grade | Desirable |
| Write clear concise documents | All grades |  |
| The ability to manage multiple tasks and projects. | All grades |  |
| Good working knowledge of cyber security risks and the mitigations required. | All grades |  |
| Ability to work with due regard to appropriate Project / Development standards | All grades |  |
| Good working knowledge of ICT security standards and requirements to ensure that all data is effectively managed. | 7, 8, 9 |  |
| Good working of knowledge of requirements such as PSN/PCI. | 7, 8, 9 |  |
| Good working knowledge of ICT infrastructure ideally including Microsoft AD group policy. | 7, 8, 9 |  |
| Good working knowledge voice and data networks ideally including Cisco firewalls. | 7, 8, 9 |  |
| Good working knowledge of business applications. | 7, 8, 9 |  |
| Good working knowledge of web based applications and web security certificates. | 7, 8, 9 |  |
| Good working knowledge of ICT security tools ideally including Nessus Vulnerability Scanner and Sophos Endpoint protection. | 7, 8, 9 |  |
| Good working knowledge of ICT security vulnerabilities of software applications, web based applications, and infrastructure. | 7, 8, 9 |  |

|  |  |  |
| --- | --- | --- |
| Behaviours | Essential | Desirable |
| Able to communicate ICT security information to non-technical staff and how it relates to their business | All grades |  |
| Work effectively under pressure | All grades |  |
| Effective problem solving skills | All grades |  |
| Self-motivated and able to work on own initiative, when required, but in the main work as part of high performing, customer focused team. | All grades |  |
| Plan and prioritise own workload ensuring that deadlines and targets are met. | All grades |  |
| Puts the customer at the heart of all solutions and approaches proposed. | All grades |  |
| Effective negotiation skills. | All grades |  |
| Smart, polite, confident. | All grades |  |
| Connect long-range visions and concepts to daily work. |  | All grades |

Note: Applicants who are disabled (as defined by law) will be guaranteed an interview if they meet the essential criteria provided that this information is noted under the relevant section of the application form.