****JOB DESCRIPTION

|  |  |  |  |
| --- | --- | --- | --- |
| Job Title | **Cyber Security Engineer** | Post Number | **F1053** |
| Grade | Career Grade 7 - 9 | Service Area | Resources |
| Special Conditions | Required to travel to various locations in response to ‘call outs’ at short notice  Required to work occasional weekends/evenings | Additional Benefits | Casual Car User |
| Authorised by | Deputy Chief Executive | Date | March 2022 |

**Job Purpose**

|  |  |
| --- | --- |
| The purpose of this role within the Council is: | To be responsible 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: | N/A |

|  |  |
| --- | --- |
| **This post is career graded. Indicative levels of responsibility at each grade are as follows** | |
| Grade 7 | Responsible for Vulnerability Scanning; Software Patching; and Supported Application Compliance. Other technical duties with support from ICT Service Manager. |
| Grade 8 | Independently responsible for all technical duties below but with support from ICT Service Manager for Investigations; Application Security; Infrastructure Security; and Web Security. |
| Grade 9 | Independently responsible for all duties above. |

|  |  |
| --- | --- |
| **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. |
| 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 OSN submissions |
| 4 | PCI Compliance:   * Review reports from PCI compliance organisation (currently Security metrics) * Act on reports and ensure any vulnerabilities are addressed within prescribed timescales * Maintain awareness for 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 and 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 | Support 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 supported applications are run on South Worcestershire ICT systems |
| 10 | Applications 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 GDPR |
| 18 | Provide technical consultancy to the service units on any ICT Security issues and developments as required |
| 19 | Ensure you approach your duties taking into consideration the principles of value for money and a flexible, customer focused approach |
| 20 | 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 outlines in ICT strategy |
| 21 | Provide accurate and timely reporting, documentation and updates to the business as required |

**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 / experience at an equivalent level) | Essential | Desirable |
| Grade 7 to 9: Degree or equivalent qualification in ICT related subject or equivalent practical experience | E |  |
| Grade 8:At least one years practical work experience of ICT security involving vulnerability scanning, investigations, compliance and reporting.  Grade 9: At least three years practical experience of ICT security involving vulnerability scanning, investigations, compliance and reporting or at least one year practical experience of ICT security, as above, in addition to at least two years practical experience of support and delivering projects in an ICT Infrastructure role | E |  |
| Grade 9: Working towards CISSP qualification | E |  |
| ITIL Foundation |  | D |

|  |  |  |
| --- | --- | --- |
| Experience | Essential | Desirable |
| Grade 9: Experience of advising at a corporate level on ICT Security | E |  |
| Grade 8:At least one years practical work experience of ICT security involving vulnerability scanning, investigations, compliance and reporting.  Grade 9: At least three years practical experience of ICT security involving vulnerability scanning, investigations, compliance and reporting or at least one year practical experience of ICT security, as above, in addition to at least two years practical experience of support and delivering projects in an ICT Infrastructure role | E |  |
| Grade 7 to 9: Good working knowledge of cyber security risks and the mitigations required | E |  |
| Grade 7 to 9: Good working knowledge of ICT Security standards and requirements | E |  |
| Grade 8 to 9: Good working knowledge of requirements such as PSN/PCI | E |  |
| Grade 8 to 9: Good working knowledge of ICT Security tools ideally including Nessus Vulnerability Scanner and Sophos Endpoint protection | E |  |
| Grade 8 to 9: Good working knowledge of ICT Security vulnerabilities of software applications, web based applications and infrastructure | E |  |
| Grade 8 to 9: Good working knowledge of ICT Infrastructure ideally including Microsoft AD group policy | E |  |
| Grade 8 to 9: Good working knowledge of voice and data networks ideally including Cisco firewalls | E |  |
| Grade 8 to 9: Good working knowledge of business applications, web based applications and web security certificates | E |  |
| Experience of working through change in a complex organisation |  | D |
| Knowledge of ICT issues at a national and local level, including national Digital by Default Strategy and place shaping |  | D |

|  |  |  |
| --- | --- | --- |
| Skills Required | Essential | Desirable |
| Grade 8 to 9: Able to identify and work independently on ICT security tasks and projects | E |  |
| Ability to work with due regard to appropriate project/development standards | E |  |
| Confident and self motivated and resilient of pressure | E |  |
| Work effectively under pressure | E |  |
| Effective problem solving skills | E |  |
| Able to write clear and concise documents | E |  |
| Self-motivated and able to work on own initiative when required but for the most part work as part of a high performing, customer focused team | E |  |
| Plan and prioritise own workload ensuring that deadline and targets are met | E |  |
| Manage multiple tasks and projects | E |  |

|  |  |  |
| --- | --- | --- |
| Behaviours | Essential | Desirable |
| Polite and respectful of others | E |  |

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.

Career Grade for Role

NOTE: Appointment to and progression through linked grades is dependent upon achieving the relevant qualifications and experience details in the Person Specification, management’s discretion as to the need to work at the higher levels to be undertaken, and the postholder’s ability to undertake such work. Normal incremental progression within the grade will apply until the postholder meets the criteria for progression to the next salary grade.

a) BASIC CRITERIA

NOTE: Applicants who are disabled (as defined by law) will be guaranteed an interview if they meet the basic criteria provided that this information is noted on the application form.

Grade 7

At appointment:

* Degree or equivalent qualification in ICT related subject AND / OR Practical experience of security in an ICT environment
* Ability to work on assigned security tasks and ICT projects under supervision.

Progress to Grade 8 subject to:

* Postholder meets criteria/experience specified for appointment to grade 8 AND
* line managers confirmation of satisfactory performance in the post/undertaking the level of responsibilities required at grade 7AND
* line managers recommendation for progression to grade 8.

Grade 8

At appointment:

* Degree or equivalent qualification in ICT related subject or equivalent practical experience.
* At least one years practical work experience of ICT security involving vulnerability scanning, investigations, compliance and reporting.
* Able to work independently on ICT security tasks assigned by manager.

**Progress to Grade 9 subject to:**

* Postholder meets criteria/experience specified for appointment to grade 9**AND**
* line managers confirmation of satisfactory performance in the post/undertaking the level of responsibilities required at grade **AND**
* line managers recommendation for progression to grade 9.

Grade 9

At appointment:

* Degree or equivalent qualification in ICT related subject or equivalent practical experience.
* Working towards CISSP qualification.
* At least three years practical experience of ICT security involving vulnerability scanning, investigations, compliance and reporting.
* Experience of advising at a corporate level on ICT security .
* Able to identify and work independently on ICT security tasks and projects.

Grades 7 to 9:

* Able to communicate ICT security information to non-technical staff and how it relates to their business.
* Work effectively under pressure
* Effective problem solving skills.
* Write clear concise documents
* Self-motivated and able to work on own initiative, when required, but in the main work as part of high performing, customer focused team.
* Plan and prioritise own workload ensuring that deadlines and targets are met.
* Manage multiple tasks and projects.