

**ROLE DESCRIPTION**

|  |  |
| --- | --- |
| **JOB TITLE** | **POST NUMBER** |
| **Cyber Security Analyst** | **R3033** |
| **DIRECTORATE** | **LOCATION** |
| Community | Hybrid working (mix of home and office working) |
| **GRADE** | **OTHER ALLOWANCES** |
| WDC9 | Casual Car User |
| **KEY WORKING RELATIONSHIPS** | **INTERNAL/EXTERNAL** |
| **Who will I be working with?**  **How will I be interacting with others?**  **This covers JE Criteria G (Relationships)** | Head of Digital and Benefits  Digital Services Manager  Infrastructure Team Leader  Network architect  Digital Services  All Council departments  Members  External Security and IT partners  Local authorities  SEGWARP  Interactions will be by internal communications. Regular “1to1” s and attending weekly meetings.  Information sharing, providing advice and guidance on cyber security matters and new trends and threats to all levels in the organisation. |
| **STATUTORY RESPONSIBILITIES/LEVEL OF ACCOUNTABILITY** | |
| **What am I accountable for?**  **What are the consequences for me or the council?**  **This covers JE Criteria D (Accountability)** | **Protect and defend**: identify, analyse and mitigate threats to IT systems and/or networks.by monitoring network activity and responding to threats. Report to management of potential of any threats to data, systems and security.  Consequences for neglect or errors for the council would include potential financial loss and reputational damage. |
| **DECISION MAKING AUTHORITY** (INDEPENDENCE) | |
| **What actions can I take independently?**  Use defensive measures and information collected from a variety of sources to identify, analyse, and report events that occur or might occur within the network to protect data, information systems and networks from threats.  Respond to security alerts to mitigate immediate and potential threats. Use mitigation, preparedness, and response and recovery approaches, as needed, to maintain information security and minimize impacts.  Developing policies that promote good security practices.  Conducting risk assessments of threats and vulnerabilities; determine deviations from acceptable configurations, enterprise or local policy; assess the level of risk; and develop and/or recommend appropriate mitigation countermeasures.  Assess training needs to maintain a cyber security culture around the council including development and testing of incident response plans.  **When do I need to involve others?**  Report to senior leadership team on cyber security threats that could have an impact to the council. This will include advice and guidance on recommended procedures or changes. | |
| **JOB PURPOSE** (COMPLEXITY) | |
| **Why does this job exist?**  Promoting and maintaining a good cyber security culture around the organisation. The role is to protect the digital infrastructure of organisations.  **How does it contribute to the Council overall?**  Keeping the council IT systems and data safe from loss, theft or encryption. | |

|  |
| --- |
| **ROLE RESPONSIBILITIES** |
| * Lead the Council’s Cyber Security response, keeping up-to-date with new threats and tools to deal with them. * Identify threats and vulnerabilities. Assess current security measures and recommend improvements in security. * Provide advice on best practice for cyber security, ensuring relevant policies and processes are up to date. * Run exercises to test organisational cyber readiness. * Maintain and promote a cyber security risk register. * Create, maintain and deliver cyber security awareness training for staff, senior leaders and members. * To undertake such other duties as the Digital Services Manager shall from time to time determine. * Support cyber security risk assessments, audits and incident management. * Assess security models to meet the current Digital Services IT standards. * Manage cyber security operations processes in accordance with organisational policies, standards and business requirements. * Development, testing and revision of Cyber Security Incident Response Plan. * Write reports, give verbal reports and presentations in the context of the cyber security role. * Review and implement recognised security frameworks such as PSN, Cyber Essentials and Cyber Assessment Framework (CAF). |
| **What other activities will I be responsible for?**  Network, Infrastructure and communication projects |
| **Will I be managing others?**  Yes, a Cyber Security Officer. |
| **Who do I report into?**  Digital Services Manager. |

|  |
| --- |
| **PROGRESSION & DEVELOPMENT** |
| **What are the development opportunities for me?**  Cyber Security, Cloud Security, Network and Communications, Incident Response, Penetration testing. |
| **How will I know I am being successful in this role?**  Through constant feedback from day to day interactions. Formal “1to1” meetings and appraisals. |
| **What is the required learning for me in this role?**  Cyber Security trends. Learning “on-the-job”.  Project Management  Attending online seminars. |

This is an outline job description designed to summarise the key responsibilities of the role and is not intended to cover every task that may be required. It may be subject to change to meet the evolving needs of the organisation.

|  |  |
| --- | --- |
| **Additional Role Requirements** | |
| Standards of Conduct | You will be required to comply with the Council’s Standing Orders and Standing Financial Instructions, and at all times deal honestly with the Council, Members, Colleagues and all those who have dealings with the Council, including customers and suppliers.  You must behave with integrity, act lawfully and demonstrate a strong commitment to ethical values.  To positively demonstrate the Wealden values yourself and to continue to build the culture of the Wealden values through the appointment, management, appraisal and development of staff (as well as third party providers). |
| Health & Safety/Risk Management | Wealden District Council’s Health & Safety Policy and other safety procedures and guidelines are deemed part of this job description. Employees must look after their own health, safety and welfare and be mindful of other persons who may be affected by their acts. Employees must co‑operate and comply with management instructions regarding H&S issues and report all accidents, incidents and problems to their supervisor, manager or other senior members of staff, in line with the H&S policies.  You will need to be compliant with the Council’s risk management policies and procedures. These describe the Council’s commitment to risk management, the recognition that our aim is to protect colleagues and visitors from harm, and stress that all colleagues have a responsibility to minimise risk. |
| Governance Standards | Comply with the relevant governance standards applicable to the Council as communicated to the post-holder from time to time. |
| Data Protection | To comply with Council Policies and the Data Protection Act in all respects, with particular relevance to the protection and use of staff and customer information. |
| Confidentiality | Council colleagues are required to ensure that information about customers and staff is safeguarded to maintain confidentiality and is kept securely in accordance with General Data Protection Regulations (GDPR), Data Protection Act 2018 (DPA18). The Council’s Data Security and Protection policy ICT policies provide guidance on how this can be achieved. |
| Communication | To encourage innovation and positive challenge through effective involvement, motivation and communication with Officers, Members, Partners and other Stakeholders, actively promoting the Council’s reputation and image as an employer of choice. |
| Digital/  Records Management | To direct the identification, development and implementation of digital and other systems and procedures which are aligned to the Council’s Drive to Digital Strategy and are shaped to reflect our customers’ and stakeholders’ needs.  To maintain Council customer and staff records (both paper and electronic) in accordance with Council policies. |
| Freedom of  Information | To provide advice and assistance to all persons who propose to make, or have made requests for information, and to ensure all requests for information are managed appropriately in accordance with Council Freedom of Information procedures. |
| Security | To comply with Council policies to ensure there is a safe and secure environment that protects Members, staff and visitors and their property, and the physical assets and the information of the organisation. |
| Other duties | Participate in such non-routine duties as elections and Emergency Planning as directed by the Chief Executive to include, where appropriate, the setup of a Rest Centre. |
| Freedom to Speak Up  (Whistleblowing) | You have responsibility for customer and staff welfare and should raise any concerns relating to a breach of Council policies and procedures with your manager or refer to HR for alternative options. |
| Environmental Impact | You will ensure compliance with the Council’s environmental management policies and procedures. These describe the Council’s commitment to climate change and carbon management, the recognition that our aim is to protect the environment and the use of natural resources that all staff have a responsibility towards. |
| Performance review | This Job Description will be used as a basis for individual performance review between you and your line manager.  The Job Description covers only the key result areas and, as such, does not intend to provide a comprehensive list of objectives. Specific objectives will be reviewed each April and may develop to meet the changing needs of the service. You will need to take due account, in the way they achieve the key result areas, of Council policies and procedures. |
| Equality and Diversity | To take responsibility and comply with the Council’s Equal Opportunities policy (which makes a commitment to promote equal opportunities and equality of all protected characteristics in Wealden), Officers’ Code of Conduct, Data Protection and other relevant policies, procedures and legislation, to ensure these are embedded and applied throughout the service in both service provision and employment issues. |

|  |
| --- |
| **PERSON SPECIFICATION** |

| **CRITERIA** | **ATTRIBUTES** | **ESSENTIAL** | **DESIRABLE** | **ASSESSED BY**  **Application Form / Interview / Practical Assessment** |
| --- | --- | --- | --- | --- |
| **Knowledge & Experience** | Strong technical skills with previous experience of working in an ICT environment. | 🗸 |  | Application Form |
| Undertaking a mentoring or coaching role and the ability to influence others at all levels. |  | 🗸 | Interview |
|  | Detailed knowledge and experience of using Microsoft software products | 🗸 |  | Application Form |
|  | In depth knowledge and experience of back-up technologies and restore strategies. | 🗸 |  | Application Form |
|  | In-depth understanding of operating systems (Windows/Linux) | 🗸 |  | Application Form |
|  | Knowledge of endpoint security concepts and cyber security | 🗸 |  | Interview |
|  | Fundamental programming/scripting capabilities (e.g. python, powershell, bash) |  | 🗸 | Interview |
|  | General knowledge of IT networking concepts, protocols and network security concepts, controls and best practices | 🗸 |  | Application Form |
|  | Knowledge of security regulations including PSN, PCI-DSS and Data Protection/GDPR | 🗸 |  | Interview |
| **Skills** | Strong analytical skills in order to interpret and analyse complex issues with proven problem solving skills particularly in relation to ICT | 🗸 |  | Application Form |
| Ability to meet deadlines and work under pressure, often independently. | 🗸 |  | Interview |
| Excellent written and verbal communication skills, appreciating the needs of different audiences. | 🗸 |  | Application Form |
|  | Ensuring that procurement of cyber services follow Wealden standards | 🗸 |  | Interview |
|  | Excellent customer-focus skills offering a proactive service showing active listening, empathy, adaptability and patience. | 🗸 |  | Interview |
|  | Ability to negotiate timescales and costs with internal service areas and external suppliers | 🗸 |  | Interview |
|  | Excellent problem-solving techniques and analysis skills | 🗸 |  | Interview |
|  | Ability to connect and engage with stakeholders | 🗸 |  | Interview |
| **Qualifications/**  **Education** | Graduate level of education in relevant related subject or professional equivalent in Cyber Security (e.g. Apprentice Level 4) | 🗸 |  | Application Form |

