Candidate Information

Position: Cyber Security Analyst
School/Department: IT Systems and Services
Reference: 21/108676
Closing Date: Wednesday 17 March 2021
Salary: £33,797 - £40,322 per annum.
Anticipated Interview Date: Thursday 1 April 2021

JOB PURPOSE:

To provide technical and administrative support for the development, maintenance and monitoring of the Cyber Security Systems used by the University.

MAJOR DUTIES:

1. Identify, deploy, configure and manage Cyber Security Systems.
2. Monitor Cyber Security Systems and Reports for indicators of compromise or breach.
3. Work with the Cyber Security Team and other technical staff to identify, report and resolve security issues and incidents.
4. Assist with Security Audits, Security Monitoring, Vulnerability Scans and Penetration Testing of University IT Systems and Infrastructure, reporting on findings and assisting with resolutions.
5. Assist in the creation of Cyber Security Policy, Procedural and Awareness documentation.
6. Research and evaluate emerging cyber security threats and possible solutions to mitigate such threats.
7. Assist in the production and analysis of monthly cyber security reports for senior management.
8. Produce weekly security vulnerability reports for the University IT community.
9. Assist in the production of the quarterly Cyber Dashboard.
10. Keep in touch with the latest trends in cyber security developments.
11. Provide specialist/professional advice, information and assistance to users – either directly or through the Helpdesk – to resolve problems and to maximise service quality, efficiency and continuity
12. Must be willing to undertake support, installation and development work outside of ‘normal’ working hours, possibly on a rota/shift.
13. Liaise with University IT Support staff on cyber security issues and provide reports to the quarterly Cyber Security Group meetings.
14. Carry out any other duties which are appropriate to the post as may be reasonably requested by senior management.

Planning and Organising:

1. Plan own work over the short to medium term with an awareness of longer term issues, in response to manager’s general instructions.
2. Contribute to larger projects as part of a project team.
3. Contribute to the planning and organisation of service changes with regard to their impact on the business of the University.
4. Develop appropriate work schedules in order to meet targets and/or turnaround times.

Resource Management Responsibilities:

1. Assist in the planning of resources within the area of responsibility to ensure that they are effectively managed and monitored.
2. Advise on the cost/benefit of new and existing technologies.
3. Assume delegated responsibilities as appropriate.
4. Manage/supervise staff where appropriate; monitoring and supporting the performance management and development of staff to ensure that individual contributions are maximised.

Internal and External Relationships:

1. Attend internal and external meetings to ensure that relevant cyber security issues are appropriately represented and reported.
2. Liaise with key contacts to ensure appropriate integration, collaboration and understanding on cyber security issues and objectives.
3. Liaise with external suppliers, consultants and other third parties, including law enforcement, government bodies/agencies and security organisations when necessary.

ESSENTIAL CRITERIA:

1. * Degree or higher degree or equivalent in Computer Science Cyber security or other related discipline. Or; * Degree or higher degree in any discipline combined with 5 years relevant professional experience in an IT Admin or Cyber Security role. Or; * HND or equivalent in Computer Science or other related discipline combined with 5 years relevant professional experience in IT Admin or Cyber Security role
2. * Three years recent relevant professional experience in IT Admin or Cyber Security role.
3. As outlined above, applicants without a degree-level qualification in Computer Science etc. must have five years relevant professional experience.
4. Applicants must demonstrate a good working knowledge and practical experience of cyber security.
5. Detailed professional knowledge in at least one of the following:
   • Networking infrastructure including DNS, DHCP, Firewalls
   • Server builds and configuration
   • MS Active Directory
   • Desktop Computing including build deployment, management and patching e.g. KACE
   • Web development and management.
6. Demonstrable interest in and knowledge of cyber security challenges and processes.
7. Demonstrable interest in and understanding of IT technology in general.
8. Working knowledge of SQL, PowerShell, Microsoft Office Access, Excel, and Word.
9. Must demonstrate ability to communicate technical information with clarity and effectiveness.
10. Must demonstrate ability to communicate effectively with colleagues and non-technical users to include all grades of staff throughout the University.
11. Must show initiative and enthusiasm.
12. Able to prioritise own work to meet deadlines.
13. Must be able to work both within a team and independently.
14. Commitment to post.
15. Able to respond flexibly to meet changing client requirements.
16. Keen to learn further relevant systems and application skills.
17. Must be willing to provide cover, as required, during critical periods and over some holiday periods as required in accordance with the needs of the Service.
18. Must be willing to undertake support, installation and development work outside of ‘normal’ working hours, possibly on a rota/shift basis.

DESIRABLE CRITERIA:

1. Microsoft Certified System Administrator (MCSA), Microsoft Certified System Engineer (MCSE) or any Microsoft Server/System/Application qualifications.
2. A cyber security qualification e.g. CISSP.
3. BCS Professional / Chartered Membership or equivalent.
4. Hold or be about to obtain relevant professional qualification.
5. Working knowledge of any of the following: - MS Windows (Server), MS Active Directory, Linux Operating Systems.
6. Ability to demonstrate practical experience with 1 or more recognised cyber security/ IT management solutions: E.g. KACE, Nessus Pro, SCOM, Splunk, WSUS.
7. Evidence of self-training or self-directed learning.
8. Proven diagnostic skills.
9. Knowledge of ISO27000 audit process.
10. Knowledge of Cyber Essentials.
11. Knowledge of Cyber Risk Management.
12. Knowledge of Cyber Incident Management.