LSC
leyton sixth form college
SUCCESS
AT A CARING COLLEGE

JOB DESCRIPTION

Job Title:	**Cybersecurity & Connectivity Engineer**
Reporting To:	**IT Manager**
Working Hours	**Full-time, 36 hours per week**
PayScale	**SC12- - £ 42,071- £44,608 including London Weighing Allowance**

Job Purpose:
As a senior technical practitioner with a proven track record, you will deliver comprehensive 1st, 2nd, and 3rd line IT support across all systems and applications provided by the college. In addition, you will take on a specialist lead role in cybersecurity, monitoring and analyzing threats using advanced tools and alerts to proactively mitigate risks and ensure compliance with evolving security standards.

Main Responsibilities:

- Provide IT support to users at 1st, 2nd, and 3rd line levels, covering all systems and applications.
- Monitor systems for potential indicators of vulnerability and compromise, using security tools and alerts.
- Categorize and respond to security alerts across all systems and networks, maintaining accurate security logs.
- Contribute to the administration, customization, and support of the college's firewall, wireless technologies, and connectivity infrastructure.
- Assist in maintaining designated VLANs and associated servers.
- Support the development and configuration of cloud-based security technologies to strengthen protection.
- Collaborate with the IT Manager on projects aimed at improving the quality, range, and robustness of ICT systems.

Main Duties:

IT Support

- Provide 1st, 2nd, and 3rd line support across the entire IT estate, ensuring timely resolution of technical issues for staff and students.

Cybersecurity Monitoring & Incident Response

- Monitor cybersecurity devices and systems to ensure optimal operation and effective response to alerts.
- Interpret reports and dashboard analytics using knowledge of security risks and the latest cyber intelligence.
- Escalate potential incidents to support engineers, collating and presenting all necessary information to the IT Manager for accurate investigations.
- Produce technical policies and procedures to maintain secure configurations of security devices and gateways against external and internal threats.

Network & Infrastructure

- Contribute to the maintenance of designated servers, switching, and control devices.
- Maintain connectivity and efficient operation of switch infrastructure, firewalls, and wireless systems.
- Customize and document the college network infrastructure, including accurate schedules of switches and ports connected to servers with color-coded cables for easy fault tracing and display port schedules for troubleshooting.
- Monitor wired and wireless traffic, access points, wireless controllers, and certification servers, ensuring secure re-issuance of certificates.

Network Segmentation & Security Zones

- Design, configure, and maintain Virtual LANs (VLANs) to ensure efficient network segmentation and optimized traffic flow.
- Implement VLAN policies to support security, performance, and compliance requirements.
- Assist in creating (DMZs) for hosting public-facing services while maintaining internal network security.
- Configure firewall rules and routing policies to secure communication between VLANs, DMZ, and internal networks.
- Maintain accurate documentation of VLAN and DMZ configurations, including IP addressing schemes, port assignments, and security controls.
- Conduct regular audits of VLAN and DMZ setups to ensure adherence to best practices and organizational security standards.
- Collaborate with cybersecurity teams to integrate VLAN and DMZ configurations with intrusion detection/prevention systems (IDS/IPS).

Cloud & Scripting Development

- Build skills in scripting and automation to contribute to the maintenance and configuration of cloud-based technologies.
- Assist in supporting Mac technology and its integration with Active Directory.

General Responsibilities:

- Contribute to the college's operational aims and objectives as outlined in the Strategic Plan
- Support the aims and ethos of the college as articulated in the Mission Statement, Compassionate Education Framework and other relevant documents
- Contribute to the college's commitment to inclusion and equality and, specifically, its ambition to be an anti-racist organisation
- Adhere to and promote college policies in line with our strong commitment to achieving equality of opportunity for students and in the employment of and care for staff
- Maintain an up to date understanding of Safeguarding Children and undertake training as required
- Maintain confidentiality and observe data protection and associated guidelines where appropriate.
- Comply with health and safety regulations associated with the post and employment at the College.
- Undertake any staff development (INSET/CPD) relevant to the needs of the post.
- Contribute to the college's quality improvement framework through participation in appraisal and performance review.
- Understand, comply and promote college policies in own area of work, and undertake any appropriate training to assist this process.
- Carry out any other duties commensurate with the grade and general responsibilities of the post.

The post holder will be expected to be available to work outside of their normal hours from time to time, to support key activities during the academic year. For example, enrolment, roadshows, open evenings, parents' evenings, etc. Advance notice would be given and appropriate time off in lieu would be negotiated.

Terms & Conditions

Full Time (36 hours per week), Monday to Friday.

Person Specification – Cybersecurity & Connectivity Engineer

*Application form (A), Task (T) or Interview (I)

Criteria for Selection	Essential/ Desirable	Method of assessment*
Qualifications and Training		
Degree in Computer Science, Cybersecurity, or related field	E	A
MCITP Server or Enterprise Administrator	D	A
CompTIA Security+ or equivalent cybersecurity certification	D	A
Experience		
Hands-on experience configuring and managing network switches (HPE, Cisco, Juniper, etc.)	E	A
Experience with firewall technologies (e.g. Palo Alto, Cisco ASA, FortiGate,)	E	A
Experience with mail filtering, MS Defender suite and other monitoring tools	E	A,T,I
Experience in using a wide range of I.T. systems and applications	D	A
PowerShell scripting skills	E	A,T,I
Familiarity with SIEM tools (e.g. Splunk, Sentinel)	E	A,I
Skills, Knowledge, understanding and abilities		
Strong analytical, reasoning and problem-solving skills	E	A,T
Excellent written and verbal communication skills	E	I
Ability to translate technical requirements into user-friendly solutions.	E	A, T
Ability to write and maintain technical documentation	E	A
Excellent time management and planning skills and the ability to work under pressure to balance conflicting demands.	E	A,I
A positive and solutions focussed approach	E	A,I
A collaborative approach, with experience of effectively working with others and supporting a team to achieve success.	E	A,I
Ability to demonstrate a flexible approach to work and changing priorities	E	A,I
Understanding of risk assessment and mitigation	E	A,T
Proactive and self-motivated	E	A, I
Values and Personal qualities		
Commitment to, and advocate for, the vision, mission and strategic priorities of LSC	E	A,T,I
Commitment to and compliance with LSC's safeguarding and health and safety principles	E	A,I
Commitment to respect and value equality and diversity, and an understanding of how this applies to own area of work	E	A,I
Commitment to own continuing personal and professional development	E	A,I