|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | **Post Details** | | | |
|  | **Job Title:** | Network Engineer L2 | **Function:** | IT Department |
|  | **Location:** | More London | **Unique Post Number:** |  |
|  | **Reports To:** | IT Network Manager | **Grade:** | MG1 |
| B | **Purpose of the Job**  The purpose of the role is to:  Install, monitor, support, maintain and develop the network infrastructure and architecture for Southeastern, including operational security and service improvement activities to keep the organisation sites connected securely to its data centres and supply partners.  The role will actively monitor the performance and security of the organisations network. Implementing and adjusting quality of service profiles to ensure network efficiency, and introducing and maintaining access controls to ensure only permitted and known network traffic is flowing between sites and supply partners. It will also cover provision of support, troubleshooting and resolving network issues, alongside providing network maintenance, system upgrades, application of service packs, patches, hotfixes, alongside the creation and improvements to security configurations. Working individually and as part of the wider network and IT team, actively monitoring and improving the security and resilience of the network, which will include input into security tool selection, implementing those tools and improving configurations.  The role will also monitor adherence to policy within the network, reporting potential breaches. It will also be involved in review of existing, or helping to create new policies and procedures, aimed to ensure all aspects of the network and its operation are continuously covered under appropriate and up to date policy and procedures.  The role will also be responsible for capacity monitoring of network devices, covering resource utilisation and highlighting changes to baselines, reporting trends, and undertaking capacity planning for the whole network.  The role will also lead or participate in the creation of architectural designs or design reviews for new and existing services, ensuring networking capacity, resilience and security are included by design from inception, and maintained throughout the lifecycle of services and sites. This could be through the participation in IT projects, or as part of the regular assurance process for sites and services already in production.  The role will work with the organisations’ network providers and support partners to ensure uptime is maximised, integrity is maintained, and network performance is optimised for all Southeastern sites. | | | |
|  |  | | | |
| C | **Principal Accountabilities** | | | |
| C1 | Pro-actively monitor the whole network estate, provide support, identify and mitigate risks and threats through monitoring network security products and protocols and report on findings. Develop and recommend short- and long-term fixes and remediations. Develop secure solutions and improvements for the ongoing operation of the overall network architecture. | | | |
| C2 | Proactively review and monitor network capacity across the organisation. Identify performance constraints, developing options to resolve them, including creation of secure solutions to improve utilisation or increase capacity when required. | | | |
| C3 | Monitor, support and improve the network security appliance estate. Create and update access controls to limit traffic flow to identified and allowed traffic between sites and partner organisations. Review and audit access policies and configurations to continually secure the implementation, ensuring optimal performance whilst maintaining and improving security. Implement changes to configurations as needed and develop secure solutions and improvements, working in conjunction with the wider team or support partner where necessary. | | | |
| C4 | Monitor, support and improve the switching estate. Review and continually improve the implementation to ensure optimal performance. Implement changes to switch configurations as needed and develop secure solutions and improvement plans. | | | |
| C5 | Monitor, support and improve the wireless implementation. Review configurations to continually secure the implementation. Implement changes to configurations as needed and design secure solutions and improvements, working in conjunction with the wider team or support partner where necessary. | | | |
| C6 | Work with the WAN Network circuit providers to ensure that circuits are performing at registered capacities, and faults and outages are resolved in line with service level agreements. This will also include managing site visits with them, ensuring site access requirements are in place, circuit installations are in the right place, and visits are conducted safely and securely, in accordance with the organisation’s health and safety requirements. | | | |
| C7  C8  C9  C10 | Work with the WAN Hardware provider to ensure that failures are replaced within agreed service level agreements.  Schedule and undertake regular upgrades to firmware for all network appliances, ensuring they remain within established tolerances.  Participate in projects: Understand requirements, design, manage and/or deliver networking solutions to support the project, incorporating adequate capacity planning and ensuring security controls are in place, whilst ensuring that existing services are not adversely affected.  Lead network security design for cloud solutions, including automation to support the organisations cloud expansion and network segmentation strategy | | | |
| C11  C12 | Recommend modifications to the network driven by updates in legal, technical or regulatory areas that affect IT network security.  Documentation of existing and new network designs, configurations, connections, access and security controls. | | | |
| C13 | Participate in an on-call escalation rota out of hours for network related incidents. | | | |
| C14 | Undertake any other activity that is commensurate with the role, as requested and agreed with management | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D | **Safety Responsibilities** | | | | |
| D1 | This post is required to undertake SAFETY CRITICAL WORK | Yes |  | No | X |
| D2 | This is a KEY SAFETY POST or nominated deputy | Yes |  | No | X |
| D3 | The holder of this post is identified as a KEY SAFETY MANAGER | Yes |  | No | X |
| D4 | The job requires competence in PERSONAL TRACK SAFETY | Yes |  | No | X |
| D5 | This job has SPECIFIC SAFETY RESPONSIBILITIES (if Yes see section D6 below) | Yes |  | No | X |
|  |  | | | | |
| D6 | The post holder has the following specific safety responsibilities: | | | | |
|  | Carrying out Planned General Inspections of the following locations:   * N/A | | | | |
|  | Acting as Fire Precautions Manager for the following locations:   * N/A | | | | |
|  | Safety Interface with the following external parties:   * N/A | | | | |
|  | Investigation of accidents occurring at the following locations or as requested by Safety & Environment:   * N/A | | | | |
| E | **Decision making Authority** | | | | |
| E1 | **N/A** | | | | |
| F | **Most Challenging and/or Difficult parts of the role** | | | | |
| F1 | Understanding how SET network interfaces with third party environments (Multi-VRF operations, BGP route policies, resilient VPN configuration incorporating automatic failover) | | | | |
| F2 | Understanding the network integration with remote supplier systems, which are predominantly IPSec based | | | | |
|  |  | | | | |

|  |  |
| --- | --- |
| G | **Person Specification** |
|  | Southeastern aims to recruit people not just for jobs but for long term careers. We want good quality, talented people with the right attitude who will stay with us.For these reasons we look for evidence of Southeastern values and behaviours in all potential staff and our existing staff looking for promotion along with the experience/knowledge, skills and behaviours relevant to the position applied for. These areWe care passionately about our people and passengers  * + we put ourselves in our passengers’ shoes to do what’s right for them   + we support our colleagues to be, feel and do their best   + we love the places we serve and do our bit for our communities and environment  We aim to be the best  * + we move with pace, we’re agile and learn from everything   + we relentlessly strive to be the best   + we are professionals with personalities  We make the difference together  * + we are answerable to each other and our passengers   + we trust each other and do what we say we will   + we are stronger together than we are as individuals   We also have identified behaviours required to be successful in leading Southeastern.  The Leading Southeastern framework details **how** we should be behaving in order to drive up performance to deliver **85 by 18**.  All shortlisted candidates seeking promotion will be assessed against this framework.  The job demands the following blend of experience/knowledge, skills and behaviours (all are essential, unless otherwise shown and will be assessed by application and/or interview/assessment) |
| G1 | Experience, Knowledge & Qualifications (including any specific safety training requirements)  * At least 5 years proven hands-on [network engineering experience](https://resources.workable.com/network-engineer-interview-questions) in a large organisation * Deep understanding of networking protocols (e.g., IPSEC, HSRP, BGP, OSPF, 802.11, QoS) * Excellent understanding of the OSI or TCP/IP model * Excellent experience with monitoring, network diagnostic and network analytics tools * Fortinet Certified Professional - Network Security (essential) * Fortinet Certified Solution Specialist - Network Security (essential) * Fortinet Certified Solution Specialist - Secure Access Service Edge (desired) * Fortinet Certified Solution Specialist – Public Cloud Security (desired) * Fortinet Certified Solution Specialist – Zero Trust Access (desired) * CCNP Enterprise (R+S/Wireless) / Security accreditation or equivalent (essential) * Experience working with network circuit service providers (essential) |
| G2 | Skills (including any specific safety critical competencies)  * Routing/switching configuration and management of Fortigate and Cisco   + Must have excellent understanding of enterprise routing protocols (BGP/OSPF/IPSEC/HSRP)   + Must have extensive experience with QOS design, implementation, and management * Aruba / HPE / Forti switching configuration and management * Cisco Nexus configuration and management * Meraki WLC configuration and management * SD-WAN deployment and configuration, management and security * An analytical mind * An ability to learn new technologies quickly * Good time management skills * An ability to follow processes * Strong documentation skills * Good communication skills – both written and verbal * Commercial and business awareness * Strong attention to detail, even when working under pressure |
| G3 | Behaviours  * Passion, enthusiasm, and expertise. * Understanding of the wider context around their work * Good written and verbal communication skills * Quality and transparency * Good prioritising skills and the ability to meet targets * Pragmatism |
| G4 | **Other** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| H | **Dimensions of role** | | | | |
| H1 | Financial – Direct: | |  | | |
| H2 | Financial – Other: | |  | | |
| H3 | Staff Responsibilities – Direct: | |  | | |
| H4 | Staff Responsibilities – Other: | |  | | |
| H5 | Any Other Statistical Data: | |  | | |
| I | **Acknowledgement** | | | | |
| I1 | Prepared By: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| I2 | Approved By (Head of Department): | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **J** | **Job Description Briefing** | | | | | |
|  | The post holder has been briefed on and understands the requirements of this Job Description and other related documents: | | | | | |
|  | Name of post holder: |  | Signature: |  | Date: |  |
|  | Name of briefing manager: |  | Signature: |  | Date: |  |
| **K** | **Nominated Deputy for Safety requirements** | | | | | |
|  | If this is a KEY SAFETY POST (D2 in Safety Details above is YES) at least one nominated deputy must be identified. The Job Holder must ensure that the Nominated Deputy(ies) receives a copy of, and is briefed on this Job Description. If there are more nominated deputies, they should sign further copies of this Job Description. | | | | | |
|  | The nominated deputy has been briefed on and understands the requirements of this Job Description and other related documents: | | | | | |
|  | Name of nominated deputy: |  | Signature: |  | Date: |  |
|  | Name of briefing manager: |  | Signature: |  | Date: |  |