Job Description

Network & Security Administrator

Grade: TBD

Reporting To: Head of ICTSS

Salary and Benefits: As per contract

Description:

The Network & Security administrator is tasked with designing, operating, securing and continuously improving the network and security infrastructure of the College. This position encompasses campus LAN and Wi-Fi, Internet connectivity, data center and disaster recovery links, Firewalls, security monitoring and secure remote access. The role is responsible for ensuring the continuity of services, forensics investigations, risk reduction and recovery planning, and infrastructure upgrades. Working under the umbrella of ICTSS, the position is responsible for coordinating with College departments and service providers to ensure the protection of College systems and data and reliable connectivity for academic and administrative needs.

Duties and Responsibilities:

The person in this role will contribute to the operation, security and ongoing improvement of the college network environment as follows:

1. Describe, install, and troubleshoot enterprise LAN, WAN and campus Wi-Fi, data center and disaster recovery connectivity using routers, switches, wireless controllers, access points and other security appliances.
2. Install and configure firewall platforms, VPNs, network segmentation and secure access controls; familiarity with Fortinet and Palo Alto technologies are very valuable.
3. Use suitable monitoring, logging and SIEM tools to monitor network performance and security; investigate alerts and identify anomalies; and coordinate prompt response to incidents.
4. Perform network security reviews and vulnerability assessments, assist with penetration testing, share vulnerabilities found and implement remediation with relevant ICT teams.
5. Use testing, change control and recovery procedures to plan and execute approved infrastructure changes, firmware updates, health checks and configuration backups.
6. Prepare and update network, device and IP inventories, security policies, standard operating procedures, incident logs and other network technical documentation.
7. Support network and network security planning, upgrades, expansion and other projects as per institutional needs and service priorities.
8. Coordinate with internet and technology providers, vendors and technical support center on service problems, escalations, warranties, renewals, quotations and technical specifications.
9. Offer advanced troubleshooting and technical advice on network and security issues, assist users and ICT staff and encourage users to be aware of good networking practice.
10. Make regular service, incident and risk reports, and participate in operational planning, auditing and development of ICTSS.

Required Skills:

1. In-depth understanding of enterprise networking protocols such as TCP/IP, subnetting, routing, switching, VLAN, STP, DNS, DHCP, WAN and wireless technologies.
2. Hands on experience in enterprise firewalls, privileged networks, HA, network segmentation and secure configuration, Fortinet/Palo Alto/Cisco experience is a Plus.
3. Knowledge on security monitoring, SIEM and log analysis, vulnerability management, threat response and security assessment practices.
4. Exposure to multiple sites or complex environments with experience in network monitoring and diagnostic, performance optimization, wireless coverage and troubleshooting.
5. Knowledge of planning and executing network and security projects, changes, maintenance and recovery.
6. Demonstrated documentation and reporting capabilities, including network diagrams, SOPs, configuration records, incident reports and technical specifications.
7. Excellent analytical and incident management skills, communication and stakeholder coordination including being able to clearly break down technical risks.
8. Independence and collaboration skills, ability to prioritise competing service needs, confidentiality and service focus.

Qualifications and Experience:

1. Bachelor's Degree from a recognized institution in computer science, computer networks, cyber security, information technology or related field. Master's is preferred.
2. Experience with network engineering, network security, and/or infrastructure administration for a minimum of 8 years with hands-on experience in enterprise networks. Experience at multiple sites or higher education is a plus.
3. Experience in relevant professional certifications, including but not limited to CCNA/CCNP, PCNSE, and Fortinet certifications is a plus.

Apply Now