

NETWORK ADMINISTRATOR -NKSTR20/2026

REPORTING TO: NETWORK MANAGER

Job Purpose: Providing network administration and technical support of network and hardware equipment. They will be responsible for ensuring that all networks and hardware is correctly installed, configured, maintained and is available and secure.

Key Responsibilities:

1. Technical Support and Administration

- Provide support on the configuration of ICT network systems and ensure efficient performance and deployment of appropriate business and support services.
- Manage the performance monitoring of ICT resources and perform advanced diagnosis and resolution of network infrastructure, software and hardware faults.
- Troubleshoot system and network problems and diagnose and solve.
- Documenting ICT infrastructure and manages entire inventory.
- Provide support, including procedural documentation instructions to repair a network fault or set up a system.
- Support the roll-out of new applications.
- Provide technical support for people using the network and day to day administration and monitoring of network use.
- Provide up to date and consistently build specifications and documentation for the core IT infrastructure and IT security infrastructure.
- Participation as a key player in the setup of new branches by installing, configuring and supporting all newly installed network equipment.
- General technical support to all computer users, both in emergency and routine.
- Troubleshooting of all network issues to identify and resolve issues affecting users.
- Liaising with the IT Network Manager regarding any technical issues that affect operations at the branch and providing recommendations on how they should best be handled.
- Lead the establishment of the networking environment by designing system configuration, directing system installation, defining, documenting and enforcing system standards.
- Design and implement new solutions and improve resilience of the current environment.
- Maximize network performance by monitoring performance, troubleshooting network problems and outages, scheduling upgrades and collaborating with network architects on network optimization.
- Undertake data network fault investigations in local and wide area environments.
- Securing network systems by establishing and enforcing policies and defining and monitoring access.
- Support and administer firewall environments in line with the Bank's IT Security policy.
- Report on network operational status by gathering and prioritizing information and managing projects.
- Upgrading data network equipment to the latest stable firmware releases.
- Remote support of on-site engineers and end users/customers during installation.
- Remote troubleshooting and fault finding if issues occur upon initial installation.

- Capacity management and audit of IP addressing and hosted devices within data centres

2. Network Security and Compliance

- Support the implementation of Next-Generation Firewalls, Intrusion Prevention Systems (IPS), and Secure Web Gateways.
- Manage the support and administration of Next-Generation Firewalls, Secure Web gateways and other network security devices
- Implement the secure remote user access and manage Virtual Private Networks (VPN) for secure remote work.
- Support the Implementation and secure partner connections and manage site to site partner vpns
- Assess network security risks, evaluate, recommend and implement as necessary.
- Support closure of audit findings within the network infrastructure

3. User Training

- Training of users where user knowledge / skills are deficient
- Providing IT training to branch ICT contacts as required on basic network configurations, and VOIP telephony issues.

Academic & Professional Qualifications

- Holder of bachelor's degree in Telecommunications, Computer Science or Information Technology related field.
- Professional technical qualifications such as CCNA
- Professional technical qualifications such as checkpoint certified security administrator (CCSA)

Experience Requirements

- 1–2 years of experience in IT networking and infrastructure,
- Advanced understanding of BGP, OSPF, MPLS, and VLANs for large-scale, complex, and high-availability LAN/WAN infrastructures.
- Knowledge of network technologies, including SD-Access and SD-WAN.
- Configuring and maintaining firewall appliances (e.g., Checkpoints & Cisco FTD) and VPN solutions to protect against threats.
- Threat Detection & Access Control: Experience with Intrusion Detection/Prevention Systems (IDS/IPS), network access control (NAC), and managing user access (RADIUS, TACACS+).
- Experience with IP Telephony and Unified Communications systems.

ALL applicants **MUST** apply online to email: recruitment@familybank.co.ke; closing date is **27th June 2026**. Canvassing will automatically disqualify the candidate. Only shortlisted candidates will be contacted.

“We are an equal opportunity employer”