JOB OBJECTIVE: **Network & Security Engineer** | C-CARE (Uganda)

Job Details

Job Grade Level	**Middle Management**	Employee Category	
Department	**IT**	Sub-Department	**IT**
Clinical/non-clinical	**Non-Clinical**	Patient Facing (Y/N)	**No**
Direct Reports (Y/N)	**Yes**	Direct Report Job Grade	**Management**

Reporting Relationships

Reporting to (Functional) **C-CARE IT Manager**

Job Summary (Main Purpose)

The Network & Security Engineer is responsible for planning, implementing, and maintaining C-Care Uganda's secure, high-performing network infrastructure. This role ensures business continuity by defending against threats, enforcing cybersecurity protocols, and optimizing connectivity across all C-Care Uganda facilities.

Main Duties/Responsibilities

Network Design & Implementation

- Design, configure, and maintain LAN/WAN networks, firewalls, VPNs, wireless access points, and routers/switches across sites.
- Implement network segmentation, VLANs, and secure remote access solutions.

Cybersecurity & Threat Management

- Monitor network activity and manage firewall rules, IDS/IPS systems, and security incident responses.
- Enforce Endpoint security, MFA, and secure access controls (LDAP, RADIUS, or AD).
- Conduct vulnerability assessments, patch management, and remediate security gaps.

Systems Monitoring & Optimization

- Utilize monitoring tools (e.g., PRTG, Forti Analyzer) to ensure optimal performance and uptime.
- Implement high availability (HA), backup connectivity, and fault tolerance solutions.

Compliance & Documentation

- Maintain and audit security policies to comply with data protection laws (e.g., HIPAA, GDPR).
- Document configurations, network topologies, and change controls.
- Participate in internal and external IT/security audits.

Support & Collaboration

- Provide L2/L3 support for escalated network and security issues.
- Work closely with application, helpdesk, and infrastructure teams on deployments and incident resolution.
- Participate in business continuity and disaster recovery planning.

Key Relationships

Internal Contacts and Purpose of Interaction

- IT Infrastructure Team – Coordinates implementation of secure systems.
- Helpdesk Team – Escalation and incident resolution.
- Clinical & Admin Teams – Ensures uninterrupted service delivery through secure access.
- Audit & Compliance Teams – Supports IT audit, risk, and compliance initiatives.

External Contacts and Purpose of Interaction

- Vendors & ISPs – Supports troubleshooting, renewals, and implementation of network/security solutions.
- OEM Support – Troubleshooting and warranty support for infrastructure assets.

Planning & Organizing Duties

Planning Cycle	Activity To Be Planned
Monthly	Firewall log review, IPS alerts, patching schedules, bandwidth utilization checks
Quarterly	Vulnerability scans, DR drills, configuration backup validation
Annual	Security policy review, infrastructure refresh planning
Long-Term Planning	Upgrade roadmap for network devices and cybersecurity infrastructure (2–3 years)

Key Skills and Competencies

Qualifications

- Degree in Information Technology, Computer Science, or related field
- Relevant certifications: Fortinet NSE 4+, CCNA/CCNP, CompTIA Security+, CEH, or equivalent.

Experience

- 3–5 years of experience in network and cybersecurity engineering.
- Experience with firewall management, IDS/IPS, VPNs, and enterprise Wi-Fi systems.
- Familiarity with healthcare IT and compliance standards is an advantage.

Knowledge & Technical Competencies

- Expertise in TCP/IP, VLANs, routing protocols (OSPF/BGP), DNS, DHCP, VPNs.
- Skilled in using Fortinet, Cisco, or equivalent platforms.
- Working knowledge of SIEM, NAC, MFA, and endpoint security tools.

Behavioral Competencies

- Proactive problem-solver and excellent communicator.
- High attention to detail and ability to work independently.
- Adaptable, with a strong focus on risk mitigation and operational continuity.