THE NAIROBI HOSPITAL

CAREER OPPORTUNITY

The Nairobi Hospital, a leading health care institution in Eastern Africa has an excellent career opportunity for an individual who possesses a passion for excellence, strong work ethic, results oriented and committed to continuous improvement. The successful candidate will be a team player with the ability to effectively add value to enabling good patient outcomes and shape best clinical and non-clinical practice in line with our Strategic Plan (2025-2029).

IT SECURITY OFFICER   **REF: TNH/HRD/ITSO/04/2025**

The IT Security Officer shall be responsible for both internal and external security hardening of systems, designing, identifying, implementing and enforcing modern security-based technologies, policies and procedures that protect The Nairobi Hospital's entire ICT infrastructure, data, information, and applications from all forms of security vulnerabilities.

Key duties and responsibilities

a) **Network and information security administration**
   1) Performing network Intrusion detection and prevention, vulnerability scanning, and monitoring.
   2) Administering centralized enterprise antivirus solution and client operating update and configuration.
   3) Performing regular vulnerability scans to find any flaws for mitigation. Administering automated security patching solutions with up-to-date security updates and hotfixes.
   4) Performing day-to-day operations and maintenance of both on-premises and cloud data center solutions.

b) **Network Security Risk Assessment for Mitigation**
   1) Performing daily health checks on systems and continuously monitoring access to network services and devices.
   2) Ensuring that security changes and improvement actions are evaluated, validated, and enforced according to the Nairobi Hospital policies and procedures.

3) Collecting and maintaining Security related data needed for purposes of monitoring trends.
4) Tracking security audit findings, assessments and recommendations for appropriate mitigation.
5) Mitigating any existing or potential security threats.
6) Creating management reports on security trends and status.

c) System Security Risk Assessment, Monitoring for Optimization

1) Securing and optimizing remote sites network and communication technologies.
2) Monitoring network performance, report and troubleshoot outages resulting from security breaches and other factors.
3) Recommending resource requirement required for cybersecurity operations.
4) Participating in security risk assessments.
5) Identifying and mitigating vulnerabilities targeting The Nairobi Hospital network and provide timely mitigating measures.
6) Developing and implementing a comprehensive plan to secure ICT Network.
7) Proactive monitoring systems usage to ensure compliance with security policies.

d) Technical Support, Troubleshooting and Capacity Building

1) Keeping up to date with emerging security trends and developments in ICT security standards and threats.
2) Documenting any security vulnerabilities and assessing extend of breaches.
3) Transferring knowledge of security skills, guides, standard operating procedures and best practices for information security to staff including non-technical audience.
4) Preparing and distributing important security alerts, or advisories to colleagues and general staff.
5) Working with external IT vendors

Knowledge, experience and qualifications required

- Bachelor of Science degree in Computer Science, Software Engineering or any other related field from a recognized institution.
- 3+ years of progressive hands-on experience in a large enterprise ICT security
- Internationally recognized security certification e.g. CompTIA Security+, CCNA Security, Microsoft Certified Security etc.
- Information Systems, Audit, Compliance and Assessment Certification are added advantages.
- EC-Council Certified Ethical Hacker Certification is an added advantage

Competencies

Technical & Behavioural competencies

- Experience in designing and implementing organization wide information security network architecture and framework.
- Experience in managing and implementing large-scale information security network projects.
- Experience in identifying and managing technology security risk.
- Up-to-date knowledge of future IP and network security technologies, equipment and their benefits.
- Systems Security Management.
- Incident Management Tools.
- LAN, WAN and Wireless Network management.
- Operating System, application and databases security configurations and Administrations.
- Storage, virtualization, backup and restore solutions for business continuity.
- Solid knowledge of various information security frameworks.
- Cybersecurity tools and techniques for Network defense.
- Brand protection including web and email.
- Routing, switching, firewall administration on a TCP/IP networking.
- Managing network services and server roles.
- Data Loss Prevention, Protection and Encryption. Knowledge of security related laws, policies, procedures, or governance relevant to cybersecurity.
- Threat Analysis and Vulnerabilities Assessment.

If your background, experience and competence match the above specifications, please send us your application (cover letter & CV/Resume) quoting the job reference number, your current remuneration, testimonials and full contact details of 3 referees, to reach the undersigned not later than **9TH May 2025.** Only shortlisted candidates will be contacted. We shall **ONLY** accept **ONLINE** applications and contact **SHORTLISTED** candidates.

*The Nairobi Hospital does **NOT** charge recruitment fees.*

Ag. Head of Human Resources
The Nairobi Hospital
P. O. Box 30026 – 00100
NAIROBI
Email: recruitment@nbihosp.org