CARITAS MICROFINANCE BANK LIMITED
VACANCIES JULY 2025

Caritas Microfinance Bank is the fastest growing Micro Finance Bank in Kenya whose vision is 'The Household Bank that Adds Value to All'. As part of our expansion strategy, we are seeking competent and qualified staff to fill the following position:

SENIOR CYBERSECURITY OFFICER JOB PURPOSE

The Senior Cybersecurity Officer is a key leadership position responsible for ensuring the security and integrity of the bank's digital infrastructure. The role involves designing, implementing, and managing advanced cybersecurity measures to protect against internal and external threats, ensuring compliance with industry regulations, and driving the continuous improvement of the bank's security posture. The ideal candidate will have a deep understanding of the latest cybersecurity technologies, frameworks, and practices, coupled with strong analytical and leadership skills.

KEY RESPONSIBILITIES

- Develop and implement the bank's cybersecurity strategy in alignment with business objectives and regulatory requirements.
- Lead and mentor the cybersecurity team to build a high-performing and responsive security function.
- Monitor access to all bank systems and maintains access control profiles on computer network and systems. Track documentation of access authorizations to all resources.
- Develop and/or maintain appropriate Segregation of Duties within and across all banking applications.
- Develop and manage the Information Security risk management strategy, framework, guideline and approach for the bank's systems and infrastructure landscape.
- Research and investigate measures that address data security risks and potential losses for reporting purposes.
- Install, modify, enhance, and maintain data system security software.
- Work on determining acceptable risk levels for the bank and ensuring the IT environments are adequately protected from potential risks and threats.
- Participate in development and implementation of the appropriate and effective controls to mitigate identified threats and risks.
- Conduct regular assessments of the cybersecurity program and recommend enhancements to senior management.
- Monitor, identify, and respond to cybersecurity threats and vulnerabilities across the bank's systems, networks, and applications.
- Develop and maintain an effective incident response plan, including coordinating investigations and reporting on security incidents.

- Conduct root cause analyses for security breaches and implement measures to prevent recurrence.
- Ensure compliance with all relevant regulatory requirements, including GDPR, PCI DSS, and local banking security standards.
- Conduct regular cybersecurity risk assessments and audits, providing recommendations for risk mitigation.
- Liaise with regulatory bodies, auditors, and other stakeholders on matters related to cybersecurity.
- Oversee the implementation of security tools, including firewalls, intrusion detection systems (IDS), endpoint protection, and data loss prevention (DLP) solutions.
- Ensure the secure configuration and patching of all IT systems and applications.
- Develop and enforce security policies, standards, and guidelines.
- Drive cybersecurity awareness programs for employees, and third-party partners.
- Conduct regular training sessions to ensure employees understand their role in maintaining the bank's security.
- Installation, configuration and upgrading of MS SQL server software and related products.
- Provide 7x24 ICT support
- Stay updated on the latest cybersecurity trends, technologies, and threat intelligence.
- Recommend and implement innovative solutions to enhance the bank's security posture.
- To perform any other duty as assigned in line with the organization goals and objective.

QUALIFICATION AND EXPERIENCE REQUIREMENTS

- Bachelor's degree in computer science, Information Technology, or related discipline
- Minimum 4 years in Information Technology with 3 years of Information and Cybersecurity relevant experience
- Information security certifications preferred: CISSP, CISM, CISA or Equivalent (Note – If not certified, willing to obtain the CISO approved IS/Cyber certification(s) in the first year of employment)
- Strong knowledge of Information Security concepts including, but not limited to, Audit Reviews, Risk Assessment, Awareness & Training, Identity Access & Management, Data Protection, Secure SDLC, Incident Management, Vulnerability Assessment, Third Party IS Assessment, Secure Configurations, Patch Management, etc.
- Thorough understanding of fundamental security related frameworks and network concepts
- Hands-on troubleshooting, analysis, and technical expertise to resolve incidents and service requests; previous experience in troubleshooting day-to-day operational processes such as security monitoring, data correlation, security operations will be an added advantage
- Ability to communicate effectively at different levels of the organization, and with various technical and business audiences.
- Excellent problem-solving abilities and analytical skills. Ability to see the big picture with high attention to critical details.
- Results oriented, can achieve desired outcomes independently and at appropriate priority levels

Interested candidates who meet the criteria above are encouraged to send their application letters and detailed CVs to: Email: recruitment@caritas-mfb.co.ke.
Kindly indicate the position title on the subject line when applying.
Closing date for application will be **28th July 2025**. Only shortlisted candidates will be contacted. For more information, please visit http://www.caritas-mfb.co.ke.