ROLE: INFORMATION SECURITY ANALYST
Reports to: Head of IT & CDO
Department: IT & CDO
Level: Senior Officer

Summary of Responsibilities:

- To support the Information and communication technology department in Information systems security Management within the bank. Security Analyst will primarily assess the adequacy of security and governance controls, evaluate threats and vulnerabilities, calculate the level of current and residual risk and apply the remedial measures to fix the identified vulnerabilities. The incumbent should plan, organize and deliver cost-effective and efficient IT security controls to protect and defend systems and information assets (business and customer data) against any internal and external threats.

Scope of Duties:

Main Functions

- Manage operations on the various security solutions.
- Manage and maintain IS security solutions.
- Monitor and ensure the proper functioning of infrastructures and services related to IS security.
- Make recommendations to improve the reliability and security of systems, networks, and applications.
- Participate in IT security analyses and the implementation of reliable security solutions.
- Perform IT security checks.
- Analyze problematic situations and intervene in problem solving.
- Any other duty assigned by the supervisor

Monitoring

- Monitor security solutions daily, analyze and report.
- Manage and monitor the Bank's firewalls and all security resources and assets
- Adopt procedures for managing alerts and escalations.
- Monitor attack levels, periodically perform penetration and vulnerability tests, track remediation actions.
- Monitor the availability and integrity of the Bank's IS.

- Review and monitor security across all systems, applications, and network infrastructure (Including Vulnerability Assessment and Penetration Testing

Operations

- Manage and maintain security solutions.
- Participate in the resolution of incidents related to security solutions.
- Develop security procedures and standards and ensure their regular updating.
- Identify and implement the recommended security controls to address the deficiencies as per industry best practices.
- Identify sources of possible errors, document them and follow up on problem resolution.
- Implement IT security infrastructure patches to be security compliant.
- Implementing both internal and external security audits as per industry best practices.
- Granting, reviewing and monitoring access on all the bank's systems
- Provide information security guidance and direction to projects and business initiatives as required. Ensure change initiatives incorporate information security requirements.
- Implementer of IT security solutions working with the local and group CISO
- Coordinate updates with other IT teams: Engage IT administrators in making configuration changes as needed.
- Develop, maintain and continuous updating of the IT Business Continuity Plan.
- Liaise and support internal and external auditors to facilitate IT audits, reviews, along with tracking and timely closure of audit outcomes.

User Assistance

- Provide support (Helpdesk) for the infrastructure, services and security applications made available to users.

Information Security Management System

- Actively participate in the various controls and the development of IS security dashboards.
- Ensure security measures are implemented as guided by the Information Security policy.
- Participate in the development of security policies and procedures.
- Introduce the relevant processes and procedures to manage Security within the Bank to help further reduce the risk of Data Breach.

Development and maintenance of IT security infrastructure

- Monitor the integration of new solutions into existing security infrastructure.
- Develop, setup, and configure security solutions where required.
- Participate in the meetings of the working groups of the "Security" projects and respect the schedule.
- Develop concepts for securing networks, systems and applications, ensure their application and monitoring.
- Communicate needs and issues on intra- and inter-team levels.
- Provide insights and recommendations on technology risk management to the bank's leadership team.
- Work directly with the Senior Executive team to design, develop and assist in the implementation of IT strategies, ensuring alignment to corporate vision/goals.

Technical Know How:

- Knowledge of security norms and standards of the security information system
- Knowledge of SIEM architectures and solutions, firewalls, intrusion detection and prevention, antimalware and spam solutions, Endpoint Detection and Response, File Integrity Monitoring, PKI, VPN, application gateways and Internet, DNS, monitoring and alerting solutions, mobile device security and management, authentication concepts, security audits, web filtering, network;
- Knowledge of Microsoft Server, Linux, Unix (Solaris) operating systems, specific security systems, network protocols.
- Recommended certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), CompTIA Security+, COBIT 5 Certifications, CRISC, CGEIT will be an added advantage

Professional skills & Experience:

- Experience in System Administration and Networks,
- Degree in computer science/ Information Security / Network / System / Telecom.
- At least 2 years of experience in Information Security Management, cybersecurity.
- Have a good sense of listening and communication skills.
- Be able to take the necessary step back to understand the queries.
- Have ease in interpersonal relationships.
- Have a sense of initiative, a sense of responsibility and the ability to work independently and in a team.
- Discipline, rigor, discretion, sense of organization and integrity.
- Good Sense of training and Strength in making proposals.
- Dynamism and diplomacy.

Submission:

All the applicants should submit their application letter, CV and Certificates not later than 08th April 2024 to email: **hr@boatanzania.com**

OR

THE HUMAN RESOURCES DEPARTMENT
BANK OF AFRICA – TANZANIA
NDC DEVELOPMENT HOUSE
OHIO / KIVUKONI STREET
P.O Box 3054
DAR ES SALAAM
TANZANIA.

NOTE: We shall communicate to only successful candidates who will meet all the requirements above.