VACANCY ANNOUNCEMENT

3. ICT Security & Compliance Officer.
Reports to: Manager Compliance
Role: The ICT Security & Compliance Officer is responsible for the development and delivery of a comprehensive information security and privacy program / policy for the Bank. As the ICT Security & Compliance Officer you are required to protect the bank information and it's infrastructure from external or internal threats and to ensure that the bank complies with statutory and regulatory requirements regarding information access, security and privacy.

Key Result Areas.

- Risk Assessment and Incident Prevention: Develop and implement an ongoing risk assessment program targeting information security and privacy matters; recommend methods for vulnerability detection and remediation, and oversee vulnerability testing.

- Policy: Coordinate the development and bank information security policies, standards and procedures. Work with key ICT and E-Banking personnel, data custodians and bank leadership in the development of such policies. Ensure that bank policies support compliance with external requirements. Oversee the dissemination of policies, standards and procedures to the bank community

- Education and training: Coordinate the development and delivery of an education and training program on information security and privacy matters for employees, and all authorized users. Should ensure that all employees are fully educated about their information security and privacy protection responsibilities.

- Compliance and Enforcement: Serve as the bank compliance officer with respect to bank information security policies and regulations while protecting the bank's information and information processing assets. He / She should as well coordinate information security efforts with the Internal Audit department.

- Incident Response: Develop and implement an incident reporting and response system to address bank Information security incidents (breaches), respond to alleged policy violations or complaints from external parties. Serve as the official bank contact point for information security, privacy and copyright infringement incidents, including relationships with law enforcement entities.

- Maintain Knowledgebase: Keep abreast of latest Information security and privacy legislation, regulations, advisories, alerts and vulnerabilities pertaining to the bank and its mission.

- Emergency Preparedness: She / He should take part in bank disaster recovery and emergency operating on a regular basis.

Minimum requirements

- Degree in Computer science or Information Technology or related discipline required
- Certification in any of the following; CISSP, MCSA, CISA, CIA is desirable together with two years' experience in Information security.
- Should have the ability to collaborate and build consensus across departments and among stakeholders who rely on information and information systems for bank operations.
- Performing ongoing risk assessments, evaluation of information security controls, and proactively maintaining compliance with industry regulations related to information security
- Experience with a wide range of relevant systems, and security monitoring and detection tools.
- Extensive ability to plan, design, develop, test, implement and monitor IT security systems
- Proactive and accountable.
- Good interpersonal and people management skills.
- Integrity, a hard worker and ability to manage change.
- Strong written and verbal communication ability.