JOB DESCRIPTION

IT Security and Database Officer

Department

Information Technology

Reports To

Chief Technology Officer

Job Purpose

The IT Security and Database Officer is responsible for safeguarding the bank's information systems and databases by implementing security controls, monitoring threats, ensuring database integrity, and maintaining high availability of critical banking systems.

Key Responsibilities

1. IT Security Responsibilities

- Monitor and respond to cybersecurity threats, alerts, and incidents
- Implement and maintain security controls including firewalls, endpoint protection, and IDS/IPS systems
- Manage user access controls and conduct periodic privilege reviews
- Conduct vulnerability assessments and support penetration testing exercises
- Ensure compliance with regulatory and internal security requirements
- Monitor system and security logs and investigate suspicious activities
- Support incident response and disaster recovery procedures
- Enforce IT security policies, standards, and best practices

2. Database Administration Responsibilities

- Administer and maintain core banking and supporting databases
- Perform database backups, recovery, and restoration testing
- Monitor database performance and optimize queries where necessary
- Ensure data integrity, availability, and confidentiality
- Manage database user accounts and access permissions
- Support application teams with database-related troubleshooting
- Implement database security hardening and patching
- Maintain database documentation and change management records

3. Governance, Risk and Compliance

- Produce periodic security and database health reports
- Monitor uptime and availability of critical banking systems
- Support internal and external audit activities
- Ensure compliance with data protection and information security policies
- Assist in risk assessments related to IT systems and databases

---

Key Performance Indicators (KPIs)

- System and database uptime availability
- Number of security incidents detected and resolved
- Backup success rate and restoration test results
- Compliance audit findings
- Patch and vulnerability remediation timelines

Required Qualifications

- Bachelor's Degree in Information Technology, Computer Science, Cybersecurity, or related field
- Relevant certifications (e.g., Security+, CEH, CISSP, Oracle, SQL Server) are an added advantage
- Must be a fully-paid up member of the Information and Communication Technology Association of Zambia (ICTAZ) and a holder of a valid practicing certificate from the Association

---

Required Experience

- Minimum of 3 years' experience in IT Security and/or Database Administration
- Experience in banking or financial services environment preferred
- Experience with database platforms (SQL Server, Oracle, MySQL, PostgreSQL)
- Experience with security monitoring tools and controls
- Understanding of Regulatory Compliance in the Banking Industry

---

Key Skills and Competencies

- Cybersecurity monitoring and incident response
- Database administration and performance tuning
- Backup and disaster recovery planning
- Access control and identity management
- Strong analytical and problem-solving skills
- Attention to detail and documentation skills

- Ability to work under pressure in a critical banking environment

---

Working Conditions

- Office-based role with occasional after-hours support
- Participation in on-call support rotation
- May be required to support disaster recovery exercises

Application Submission:

Interested candidates should submit to: jobs@ictaz.org.zm

Application Deadline: 15th April 2026