INTERNAL ADVERTISEMENT

A vacancy exists for an IT Infrastructure and Cybersecurity Manager in Johannesburg.

You will be responsible for the planning, installation, maintenance, and upgrade of IT systems and personnel. The monitoring off all channels through, which information flows into and out of the organisation's information network. You are responsible for observing all of the operations occurring across the network and managing the infrastructure that facilitates those operations. In short you will be responsible for the CIA Triad:

- **Data Integrity** - information is kept accurate and consistent unless authorized changes are made
- **Availability** - Availability is maintained when all components of the information system are working properly
- **Confidentiality** - protection of information from unauthorized access

Key responsibilities:

Infrastructure Management

- Responsible for the planning, installation, maintenance, and upgrade of IT systems
- Design and execute short plus long term strategic plans to assure infrastructure capacity attains current and future needs
- Develop, execute and oversee procedures, policies and related training plans for project management and infrastructure administration
- Manage and establish priorities for maintenance, design, development and analysis of entire infrastructure systems inclusive of LANs, WANs, internet, security and wireless implementations
- Conduct research and recommend changes in services, products, protocols and standards to support development efforts and infrastructure procurement
- Supervise data centres, direct and utilize knowledge on best practices in area related to infrastructure
- Define and manage BCM and IT Disaster Recovery Strategy for organization
- Define software and hardware standards in collaboration with stakeholders and owners
- Test server performance and provide network presentation statistics
- Report and prepare strategies to maintain server infrastructure
- Ensure apt security levels on network, infrastructure and servers are maintained
- Direct and administer conditional network analysts plus technicians to provide leadership and direction
- Ensure to practice IT asset management inclusive of component inventory maintenance and associated documentation
- Negotiate with outsourcers, vendors and contractors for infrastructure-specific products and secure services
- Perform feasibility studies for different upgrade projects, conversions and improvements
- Implement IT continuous improvement programs

- Manages a dynamic team of individuals, constantly searching for creative ways to elevate the capabilities of technology systems to meet business needs
- Participate in the budget process
- Designing and implementation of cloud adoption strategy
- Annual management of renewal process and ensuring in time compliance
- Cloud migration and implementation

System Availability

- Maintaining supporting hardware and software applications to ensure that end user applications and products are available
- Resolving system and hardware problems that arise to ensure the minimum downtime on the system
- Ensuring that end users are advised when the system has experienced problems and they will not be able to use the system
- Backing up of resources to ensure that information is available, should the system fail and needs to be restored
- Crisis management - keeping stakeholders informed and actively working with teams to return service in the shortest possible timeframe

Cybersecurity Requirements

- Understanding of relevant cyber, information and cloud security related laws and regulations
- Monitor all operations and infrastructure
- Maintain all security tools and technology
- Monitor internal and external policy compliance
- Monitor regulation compliance
    - Scheduling for ASV scans and internal vulnerability scans, remediating findings and ensuring accurate & timely reporting to satisfy PCI DSS requirements.
    - Regular account auditing, and all other PCI DSS requirements that needs to be met
- Work to reduce risk
    - User awareness training
    - Applying patches in timely fashion
    - User access levels are correct
    - Updating Firewalls, EDR, etc.
- Implement new technology
- Audit policies and controls continuously
- Ensure Cybersecurity stays on the organisational radar
- Regularly test the Security Incident Response plan
- Transparency to the Executive team

Risk and Compliance

- Remediating audit items by putting measures in place to prevent the reoccurrence of findings
- Ensuring user compliance with acceptable usage policies related to internet searches and size constraints of information sent
- Ensuring that there is an IT infrastructure in place outside of the business premises to ensure Business Continuity
- Ensuring that the infrastructure is maintained should there be damage to the company premises and existing internal IT infrastructure
- Ensuring that all servers are replicated and that regular (daily) backups take place
- Review changes as part of the Change Approval Board (CAB)

- Participate in various internal and external audits (ITGC, PCI)

Project delivery

- Being involved in projects that are designed to improve the existing environment to facilitate delivery or to transition the project into production
- Ensuring that the security related to the project is in place
- Interacting with business, vendors and staff at various levels to facilitate the implementation of approved projects

Vendor management

- Meeting with key suppliers such on a monthly basis and smaller suppliers on an annual or quarterly basis
- Ensuring that escalations required take place
- Commenting on SLAs when they are being drawn up
- Enforcing SLAs with vendors and for clients
- Ensuring that new requirements are managed with vendors, particularly when exploring potential solutions and obtaining costs from vendors

In order to be considered for the position, the following requirements must be met:

- Matric
- Completed BSC Computer Science or BCom (IT)
- ITIL Certified
- COBIT
- CISM (Certified Information Security Manager) and CISSP (Certified Information Systems Security Professional) would be an advantage
- Broad knowledge of hardware, networking, cybersecurity, vulnerability management, and cloud migration
- Working knowledge of Kubernetes implementation, support and design
- Min 5 years experience in IT Infrastructure and IT System administration
- Min 5 years experience leading an IT infrastructure team
- Min 3 years experience in Cybersecurity
- PCI DSS Requirement knowledge
- Security policies, security procedures, security design and implementation
- In depth understanding of infrastructure and network architecture and design
- Management of Windows and Linux environments
- SLA Management
- Vendor & Supplier Management
- HR Experience including: Team Creation, Motivation and Performance Management
- Finance for Non-Finance Manager (budgeting etc.)
- Firewalls
- IDS/IPS
- Endpoint Security Solutions
- Access Control Systems
- Set-up Requirements i.e. Desk, PC, Laptop etc.

Behavioral Competencies:

- Planning & Organising
- Communication & Impact
- Customer Focus
- Problem-solving
- Initiating Action
- Building a Successful Team
- Coaching & Developing Others
- Financial Acumen
- Results Orientation
- Adaptability
- Engagement Readiness
- Leadership Disposition
- Coping with stress / change