VACANCY

Postbank
Your Bank

JOB TITLE	**:**	**Head: IT Security**
REPORTS TO	**:**	**General Manager: IT Governance**
BUSINESS UNIT	**:**	**IT**
LOCATION	**:**	**HEAD OFFFICE: PRETORIA**
POSITION STATUS	**:**	**Permanent**
POSITION GRADE	**:**	**D5**

Purpose of the Job

The Head: IT Security is responsible for leading the bank's cyber security, information security, cryptography, security engineering and security operations capability to protect customer information, payment systems, card environments, digital channels, banking platforms and South African Social Security Agency payment services. Define and manage security strategies, standards, controls, monitoring practices and cyber resilience plans to reduce the likelihood and impact of cyber threats, ransomware, insider threats, unauthorised access, identity compromise, privilege abuse, data loss, service disruption and technology compromise. Direct specialist security teams to design, implement and monitor security controls across infrastructure, applications, networks, cloud services, Microsoft 365 services, endpoints, encryption environments, payment and card environments, third party services and user access. Provide the bank's senior information security authority, incident response leadership, cyber risk reporting and security assurance to maintain regulatory compliance, operational resilience, audit readiness and public confidence in the bank.

Job Responsibilities

Cyber and Information Security Strategy

- Define the bank's cyber and information security strategy to protect critical technology services, customer information and payment environments
- Own the cyber security strategy, operating model, control roadmap and executive cyber-risk reporting for ransomware, identity compromise, payment-system threats, insider threats and data leakage risk
- Set security principles, standards and control requirements to align security practices with risk appetite, regulatory obligations and technology governance requirements
- Develop the security operating model, control roadmap and cyber resilience plan to strengthen prevention, detection, response and recovery capability
- Review security risks, emerging threats and control maturity to prioritise security improvements and investment decision
- Report security posture, key risks and improvement progress to governance forums to support informed oversight and accountability

Senior Security Authority and Governance

- Act as the bank's senior in house information security authority to provide practical and authoritative security guidance
- Advise executive leadership, governance structures, risk forums and audit stakeholders on cyber risk, resilience and security investment priorities
- Define security policies, standards, metrics and reporting routines to support evidence-based decision making
- Assess material cyber risks, control gaps, residual risks and compensating controls to support risk treatment or risk acceptance decisions
- Promote security practices that balance risk reduction, operational continuity, customer access and business realities

Security Architecture and Engineering

- Direct security design requirements across infrastructure, applications, networks, cloud services, endpoints, databases and integration platforms to reduce technology exposure
- Review solution designs, technical changes, architecture decisions and vendor proposals to confirm alignment with approved security standards before implementation
- Guide security engineering activities to implement identity, access, network, endpoint, application and data protection controls

- Validate security configurations and control effectiveness across critical platforms to reduce misconfiguration and unauthorised access risk
- Support secure technology delivery for banking platforms, payment systems, card environments, digital channels and South African Social Security Agency payment service

Security Operations and Cyber Incident Response

- Lead security monitoring capability to detect, assess and respond to cyber threats across technology environments
- Direct investigation of security alerts, vulnerabilities, phishing attacks, privileged account compromise, suspected data loss and ransomware events to contain impact and restore secure operations
- Lead Security Operations Centre (SOC), Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), threat monitoring, detection engineering, phishing response, privileged account compromise and post incident lessons learned
- Develop cyber incident response plans, escalation protocols and playbooks to support timely and coordinated response
- Coordinate incident response with technology, risk, compliance, legal, communications, vendors and executive stakeholders to manage business and regulatory impact
- Review incident lessons learned to strengthen security controls, monitoring rules, recovery readiness and response procedures

Identity Privileged Access and Data Protection

- Direct identity and access management controls to confirm that user access aligns with role requirements, segregation of duties and least privilege principles
- Oversee privileged access governance, service account control, administrative access review, access monitoring and trusted identity recovery to reduce compromise risk
- Strengthen data protection controls to reduce the risk of unauthorised disclosure, loss, alteration or misuse of customer and bank information
- Manage security testing, penetration testing and control assurance activities to identify exploitable weaknesses before they affect operations
- Track remediation actions for access, identity, data protection and security findings to improve control maturity and reduce residual risk

Cryptography and Key Management

- Define cryptography standards and key management procedures to protect payment systems, card environments, customer data and sensitive banking transactions
- Oversee Hardware Security Module administration, encryption controls and key lifecycle management to maintain secure cryptographic operations
- Monitor privileged access to cryptographic systems to reduce unauthorised access and key compromise risk
- Validate compliance with payment security, card security, encryption and key management requirements to support secure transaction processing
- Review cryptographic control exceptions and operational risks to drive corrective action and maintain trust in payment services

Cyber Resilience and Recovery Readiness

- Direct cyber resilience planning to support secure recovery from ransomware, destructive attacks, data compromise and service disruption
- Review backup protection, recovery validation, clean restoration procedures, business integrity checks to support safe service restoration, ransomware-oriented recovery controls, backup protection, clean restoration decision-making and business integrity checks after cyber incidents
- Coordinate cyber recovery planning with infrastructure, cloud, application, database, operations and continuity teams to strengthen recovery readiness
- Support disaster recovery tests, cyber simulation exercises and recovery validation activities to confirm response capability and evidence readiness

- Report recovery gaps, resilience risks and remediation progress to governance forums to support informed decision making

Cloud Endpoint and Digital Security

- Direct cloud, endpoint, email, collaboration platform and digital channel security controls to protect customer facing and productivity environments
- Review cloud configuration, conditional access, mailbox security, endpoint protection and internet facing platform controls to reduce attack paths
- Coordinate security monitoring across cloud services, digital channels, card services and critical banking platforms to support risk based protection
- Track vulnerabilities, misconfigurations and control gaps across cloud and endpoint environments to support timely remediation
- Support secure adoption of new technology, outsourcing arrangements and cloud services through practical security input
- Microsoft 365 security, mailbox compromise response, conditional access, collaboration-platform abuse and internet-facing platform hardening

Regulatory Compliance and Security Assurance

- Monitor security compliance against applicable legislation, regulatory requirements, industry standards and internal policies to support assurance readiness
- Maintain security evidence, control records and compliance reports to support audit, regulatory and management review processes
- Coordinate responses to security audit findings, regulatory observations and control weaknesses to support timely closure
- Engage internal audit, external audit, risk, compliance and regulators on security matters to address findings and improve the control environment
- Promote secure ways of working across technology teams and third party providers to strengthen accountability for security outcomes
- Lead Payment Card Industry Data Security Standard (PCI DSS), Payment Card Industry Personal Identification Number Security Requirements (PCI PIN), Protection of Personal Information Act (POPIA), South African Reserve Bank (SARB), Payment Association of South Africa (PASA) related security expectations, internal audit, external audit and Auditor General South Africa (AGSA) related evidence requirements

Third Party Security and Governance Coordination

- Oversee third party cyber risk across security service providers, cloud providers, payment integrations, vendor connectivity and outsourced security functions
- Review vendor security controls, service commitments and incident response obligations to support secure external service delivery
- Challenge vendor performance where recurring incidents, weak controls or poor response quality increase security risk
- Provide senior security advice into major projects, architecture forums, outsourcing decisions, new technology adoption and cloud migration decisions
- Communicate security risks, control gaps and remediation priorities clearly to support transparent stakeholder management

Financial Management

- Compile security budget inputs and forecasts to support planned investment in security tools, services and specialist capability
- Monitor security expenditure against approved budgets to manage costs within allocated financial parameters
- Assess security investment options to balance risk reduction, compliance requirements, operational resilience and value for money
- Track benefits from security initiatives to demonstrate improved control effectiveness and reduced technology risk

People Management

- Clarify role expectations, priorities and standards for direct reports to align delivery with security objectives
- Lead performance planning, review and feedback processes to support accountability and deliver
- Coach and mentor direct reports to build capability in cyber security, cryptography, security engineering, security administration and Hardware Security Module key administration
- Allocate work, manage capacity and monitor delivery timeframes to maintain effective functional performance
- Support recruitment, onboarding, development and succession planning to maintain a capable and sustainable security team
- Address conduct, performance and attendance matters in line with Human Resources policies and labour legislation

Qualifications and Experience

- Bachelor's Degree in Computer Science, Information Systems, Cyber Security, Computer Engineering or related discipline (NQF Level 7)
- Certificate in Cyber Security, Information Security Management, Network Security, Payment Security or Information Technology Governance (NQF Level 6)
- Leadership Development Programme
- 10 Years Experience in the Information Technology industry
- 8 Years Experience in cyber security, information security, security operations, cyber risk or security engineering
- 5 Years Experience in banking technology, payment systems, card environments, digital channels or regulated financial services security
- 5 Years Experience in leading cyber security teams, security governance forums, cyber resilience planning and incident response activities

Ideal

- Post Graduate Degree in Computer Science, Information Systems, Cyber Security, Cyber Risk, Technology Governance or related discipline (NQF Level 8)
- Advanced Certificate in Information Security Management, Cyber Risk Management, Security Architecture, Security Audit or Information Technology Governance (NQF Level 6)
- Advanced Certificate in Payment Security, Data Protection, Security Operations, Cryptography Management or Information Security Audit (NQF Level 6)

Advantageous

- 5 Years Experience in cryptography, Hardware Security Module administration, key management, payment security or card security environment
- 3 Years Experience in Payment Card Industry Data Security Standards, Payment Card Industry Personal Identification Number requirements, Protection of Personal Information Act South African Reserve Bank, Payment Association of South Africa or security audit compliance environments
- 3 Years Experience in third party cyber risk management, managed security service governance, cyber maturity improvement or security operating model implementation

Special requirements

May be required to provide standby or incident support for major cyber security incidents, ransomware events, suspected data compromise, payment security incidents, critical system changes, disaster recovery tests, cyber recovery exercises, regulatory reviews or urgent security events

How to Apply

If you wish to apply and meet the requirements, please forward your Curriculum Vitae (CV) to recruitment**NM**@postbank.co.za Please indicate in the subject line the position you are applying for. To view the full position specification, log on to www.postbank.co.za and click on Careers.

Closing Date

11 November 2026

Disclaimers

The South African Postbank SOC Limited is committed to the achievement and maintenance of diversity and equity in employment, especially with regard to race, gender and disability. In compliance with the banks employment equity plans, first preference will be given to candidates from designated groups. Correspondence will be limited to short listed candidates only.

If you do not hear from the South African Postbank SOC Limited or its Agent within 3 months of this advertisement, please accept that your application has been unsuccessful. The South African Postbank SOC Limited reserves the right not to fill the positions or to re-advertise the positions at any time.

POPIA provides that everyone has the right to privacy and it includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. By applying for employment you consent to the processing of your personal information with Postbank. Your personal information and any attached text or documentation are retained by Postbank for a period in accordance with relevant data legislation.