Reg Name: Postbank (SOC) Ltd
Registration number: 2017/177755/30
NPC Building, Jeff Masemola Street, Pretoria, 0002: PO Box 10 000, Pretoria, 0001

REQUEST FOR BIDS/PROPOSALS

RFB/P REF. NO:	**04/06/26-27**
DESCRIPTION	**The appointment of a qualified and experienced service provider to deliver comprehensive Information Security and Cybersecurity services for a period of three (3) years.**
RFB/P ISSUING DATE	21 August 2026
NON-COMPULSORY BRIEFING SESSION	Date: 31 August 2026 at 11h00 am **Microsoft Teams meeting** **Join:** https://teams.microsoft.com/meet/353842123818395?p=T8FEPcWgvOAntPiWWq Meeting ID: 353 842 123 818 395 Passcode: M8hs2Ye6
RFB/P CLOSING DETAILS	Date: 18 September 2026 Time: 11:00 am
RFB/P SUBMISSION ADDRESS	RFP@PostBank.co.za
RFB/P VALIDITY PERIOD	**180 Days** from the Closing Date
ENQUIRIES **CLOSING DATE**	Vusi Maditsi: Vusi.Maditsi@postbank.co.za Thabo Mokhabi: Thabo.Mokhabi@postbank.co.za 03 September 2026 at 16h30

PART A
INVITATION TO BID
SBD1

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE (*NAME OF DEPARTMENT/ PUBLIC ENTITY*)					
BID NUMBER:	**04/06/26-27**	CLOSING DATE:	**18 SEPTEMBER 2026**	CLOSING TIME:	**11:00 AM**
DESCRIPTION	**THE APPOINTMENT OF A QUALIFIED AND EXPERIENCED SERVICE PROVIDER TO DELIVER COMPREHENSIVE INFORMATION SECURITY AND CYBERSECURITY SERVICES FOR A PERIOD OF THREE (3) YEARS.**				
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT *(STREET ADDRESS)*					
SUBMISSION IS TO BE SUBMITTED TO THE EMAIL ADDRESS STIPULATED ON THE COVER PAGE					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO:					
CONTACT PERSON	**VUSI MADITSI**				
E-MAIL ADDRESS	**VUSI.MADITSI@POSTBANK.CO.ZA**				
SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					
SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		**OR**	CENTRAL SUPPLIER DATABASE No:	MAAA
1ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES OFFERED?	☐Yes ☐No [IF YES ENCLOSE PROOF]		**2**ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES OFFERED?	☐Yes ☐No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]	

QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS

IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? ☐ YES ☐ NO

DOES THE ENTITY HAVE A BRANCH IN THE RSA? ☐ YES ☐ NO

DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA? ☐ YES ☐ NO

DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA? ☐ YES ☐ NO

IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION? ☐ YES ☐ NO

IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 BELOW.

PART B

TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:
1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
1.2. **ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED (NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT.**
1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
1.4. **THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).**
2. TAX COMPLIANCE REQUIREMENTS
2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
2.2 BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.
2.3 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE WWW.SARS.GOV.ZA.
2.4 BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
2.5 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED; EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
2.6 WHERE NO TCS PIN IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.
2.7 NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE."

NB: FAILURE TO PROVIDE / OR COMPLY WITH ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

SIGNATURE OF BIDDER:……

CAPACITY UNDER WHICH THIS BID IS SIGNED:……

(Proof of authority must be submitted e.g. company resolution)

DATE:

CONTENTS

SECTION 1 5
BIDDER'S DETAILS 5
SECTION 2 6
BID TERMS OF REFERENCE 6
SECTION 3 8
SPECIFICATION 9
SECTION 4 9
PRICING SCHEDULE/COSTING MODEL 15
SECTION 5 15
STANDARD BID DOCUMENTS (SBDs) 18
SECTION 6 18
GOVERNMENT PROCUREMENT: GENERAL CONDITIONS OF CONTRACT – JULY 2011 26

SECTION 1

BIDDER'S DETAILS

1. Bidding structure

Indicate the type of bidding structure by marking with an 'X':	
Individual bidder	
Joint Venture	
Consortium	
Subcontractors	
If the bid is submitted as a Consortium or Joint Venture or Sub Contracting, list the members of such Consortium or Joint Venture and Sub Contractors below:	
1.	
2.	
3.	
4.	

1.2 Entity Directorship

No.	Director name	Identity number
1.		
2.		
3.		
4.		

1.3 Entity Ownership

Ownership Category	% of Ownership
Black or Historically Disadvantage Individual Owned	

I certify that the information furnished on this form is true and correct.
I further accept that, in addition to cancellation of a contract, action may be taken against me should this declaration prove to be false.

_____

Name of bidder (duly authorised)

_____

Signature of bidder

_____

Date

_____

Capacity under which this bid is signed

SECTION 2
BID TERMS OF REFERENCE

2. General rules and instructions

2.1 Precedence of documents

2.1.1 This RFB/P consists of a number of sections (see list). Where there is a contradiction in terms between the clauses, phrases, words, stipulations or terms and herein referred to generally as stipulations in this RFB/P and the stipulations in any other document attached hereto, or the RFB/P submitted hereto, the relevant stipulations in this RFB/P shall take precedence.

2.1.2 Where this RFB/P is silent on any matter, the relevant stipulations addressing such matter and which appear in the PPPFA shall take precedence. Bidders shall refrain from incorporating any additional stipulations in its proposal submitted in terms hereof other than in the form of a clearly marked recommendation that POSTBANK may in its sole discretion elect to import or to ignore. Any such inclusion shall not be used for any purpose of interpretation unless it has been so imported or acknowledged by POSTBANK.

2.1.3 It is acknowledged that all stipulations in the PPPFA are not equally applicable to all matters addressed in this RFB/P. It, however, remains the exclusive domain and election of POSTBANK as to which of these stipulations are applicable and to what extent. Bidders are hereby acknowledging that the decision of POSTBANK in this regard is final and binding. The onus to enquire and obtain clarity in this regard rests with the Bidder(s). The Bidder(s) shall take care to restrict its enquiries in this regard to the most reasonable interpretations required to ensure the necessary consensus.

2.2 Preferential procurement reform

2.2.1 POSTBANK supports B-BBEE as an essential ingredient of its business. In accordance with government policy, POSTBANK insists that the private sector demonstrates its commitment and track record to B-BBEE in the areas of ownership (shareholding), skills transfer, employment equity and procurement practices (SMME Development) etc.

2.2.2 POSTBANK shall apply the principles of the Preferential Procurement Policy Framework Act, (Act No. 5 of 2000) to this proposal read together with the Preferential Regulations, 2022.

2.4 Objection to brand specific requirements

2.4.1 Any bidder who has reasons to believe that the RFB/P specification is based on a specific brand must inform POSTBANK within seven (7) days after the publication of the RFB/P.

2.5 Instructions for submitting bids

2.5.1 Bid responses must be submitted to the email address as stipulated on the cover page

SECTION 3

3. Special Conditions of the Bid

3.1 POSTBANK shall not make upfront payment.

3.2 The preparation of response shall be made without obligation to acquire any of the items included in any bidder's proposal or to select any proposal.

3.3 POSTBANK may request written clarification regarding any aspect of this proposal. The bidders must supply the requested information in writing within the specified time frames after the request has been made, otherwise the proposal shall be disqualified.

3.4 POSTBANK reserves the right to; cancel or reject any proposal and not to award the proposal to the lowest bidder or award parts of the proposal to different bidders, or not to award the proposal at all.

3.5 By submitting a proposal in response to this RFB/P, the bidders accept the evaluation criteria as it stands.

3.6 Where applicable, POSTBANK reserves the right to conduct benchmarks on product/services offered during and after the evaluation.

3.7 Failure or neglect by either party to (at any time) enforce any of the provisions of this proposal shall not, in any manner, be construed to be a waiver of any of that party's right in that regard and in terms of this proposal. Such failure or neglect shall not, in any manner, affect the continued, unaltered validity of this proposal, or prejudice the right of that party to institute subsequent action.

3.8 Should the bidder change any wording or phrase in this document, the RFB/P shall be evaluated as though no change has been affected and the original wording or phrasing shall be used.

3.9 This RFB/P is subject to Government Procurement: General Contract Conditions – July 2011, Special Contract Conditions and any other contract conditions to be finalised during contracting.

3.10 La Postbank reserves the right to:

3.10.1 Verify any information supplied.

3.10.2 Not accept any quotation.

3.10.3 Cancel or re-issue the tender at its sole discretion.

SECTION 4

SPECIFICATION

1. Introduction

Postbank seeks to appoint a suitably qualified and experienced service provider to deliver comprehensive Information Security and Cybersecurity services for a period of three (3) years. The objective is to ensure that Postbank's critical banking infrastructure and office productivity environments are fully protected against cyber threats, including ransomware, insider threats, data breaches, and service disruptions.

The appointed provider will operate as a strategic partner, supporting both the enhancement of Postbank's cyber resilience posture and the internal development of Postbank's Information Security function.

Thus, the main objective of this procurement is to appoint a strategic cybersecurity partner capable of materially strengthening Postbank's resilience against cyber-attacks, including destructive ransomware, identity compromise, data exfiltration, insider threats, attacks on banking and payment systems, and attacks affecting office productivity and corporate technology environments

2. Objective of the Requirement

The following are the overarching objectives of this engagement:

- To secure Postbank's banking and corporate IT environments against current and emerging cyber threats.
- To implement a proactive threat detection, monitoring, and incident response capability and establish a security operations center (SOC).
- To ensure compliance with SARB, PASA, PCI DSS, POPIA, and ISO/ IEC 27001 standards.
- To establish a three-year cybersecurity maturity roadmap aligned to SARB's Cybersecurity Maturity Framework.
- To strengthen internal capacity through skills transfer, mentorship, and governance model establishment.
- To require the successful bidder to provide a Postbank-specific Cyber Defense and Ransomware Protection Strategy covering prevention, detection, containment, eradication, recovery, recovery validation, crisis coordination, and continuous improvement across banking systems, office productivity platforms, endpoints, identities, networks, data, backups, cloud environments, and critical third-party integrations.
- To establish a cyber resilience capability that can withstand and recover from destructive ransomware attacks, account compromise, data exfiltration, privilege abuse, and attacks affecting both banking systems and corporate IT services.
- To implement a recovery assurance model that includes immutable or otherwise tamper-resistant backups, isolated recovery capability, recovery validation, and business/ data integrity checks following a cyber incident.
- To secure Postbank's critical banking systems, payment systems, card systems,

Automatic teller machine (ATM) infrastructure, internet-facing applications, and office productivity environments using a risk-based, crown-jewel-focused approach.

- More specifically, this bid aims to achieve the following detailed additional objectives: Secure identity, access, and privileged accounts with strict governance and controls.
- Safeguard email, communication channels, and online banking services from phishing and malware.
- Deliver continuous penetration testing and remediation, vulnerability, and patch management to reduce exposure to cyber risks. Postbank or any other agent acting on the bank's behalf will run scans and propose remediation, while the successful bidder retains responsibility to close vulnerabilities within SLA timelines.
- Provide knowledge transfer regularly, the performance of which will be assessed and reviewed monthly.
- Provide monthly updates of progress and status of knowledge transfer and topics covered in the reporting period.
- Provide threat intelligence and threat hunting capabilities
- Provide Incident Response and Forensics

The bidder must provide a migration package upon the contract's expiration. that includes all necessary data, configurations, and documentation required to transition services seamlessly to another provider or in-house operations upon contract expiry

3. Scope of Work

The appointed service provider will deliver managed cybersecurity services covering the following core areas:

3.1 Security Operations Centre (SOC)

- The bidder shall establish, operate, and maintain a fully managed 24/7 Security Operations Center (SOC) dedicated to supporting Postbank's cybersecurity operations.
- The bidder shall host the SOC within its own facilities and ensure that the hosting environment remains fully compliant with PCI DSS requirements throughout the contract period.
- Postbank reserves the right to relocate the SOC to its own premises at any stage during the contract. Should Postbank elect to do so, no hosting fees shall be payable for bidder-provided facilities.
- A minimum of three (3) months' written notice shall be provided before termination of any hosting arrangement.
- The bidder should provide continuous monitoring, detection, investigation, containment, response, and recovery services across Postbank's endpoints, networks, applications, cloud environments, and critical banking systems.
- The bidder shall deploy and manage Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) platforms capable of collecting, correlating, and analyzing security events from all relevant Postbank technology environments.
- The bidder shall maintain documented ransomware defense procedures that clearly define early warning indicators, account compromise triggers, containment actions, escalation requirements, communication protocols, executive reporting requirements,

recovery decision points, and restoration procedures.

- The bidder shall provide a clean-room cyber recovery capability that enables Postbank to recover critical services in a trusted environment following a major cyber incident.
- The bidder shall develop, maintain, and continuously improve detection use cases for ransomware activity, privilege escalation, data exfiltration, account compromise, malicious insider activity, suspicious administrative actions, mailbox compromise, OAuth abuse, and lateral movement techniques.
- All SOC playbooks, response procedures, and escalation processes shall be customized for Postbank's operating environment and approved by Postbank before implementation.
- The bidder should conduct forensic investigations following security incidents and provide detailed root cause analysis reports, evidence preservation, and recommendations to prevent recurrence.
- The bidder shall provide monthly operational reports and quarterly executive dashboards that clearly demonstrate the threat landscape, attack trends, incident response performance, control effectiveness, business impact, and recommended improvement actions.
- The bidder shall support Postbank's regulatory reporting obligations by providing comprehensive evidence packs, forensic findings, timelines, and technical analysis within agreed service levels.

3.2 Endpoint Security and Extended Detection and Response (XDR)

- The bidder shall deploy, manage, and continuously optimize a Next-Generation Endpoint Detection and Response (EDR/XDR) solution across all Postbank servers, workstations, laptops, ATMs, virtual machines, cloud-hosted workloads, and other designated endpoints.
- The bidder shall provide continuous monitoring, threat detection, threat containment, and automated response capabilities for malware, ransomware, advanced persistent threats, insider threats, and unauthorized system activities.
- The bidder shall perform server hardening, secure configuration management, vulnerability scanning, and compliance validation in accordance with industry best practices and Postbank security standards.
- The bidder shall implement and manage multi-cloud security controls across AWS, Microsoft Azure, and Google Cloud Platform environments using Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) technologies.
- The bidder shall provide comprehensive protection for Microsoft 365, including Exchange Online, Teams, SharePoint, OneDrive, and associated collaboration services. Controls shall include tenant hardening, anti-phishing protection, business email compromise prevention, OAuth governance, detection of suspicious mailbox activity, and compromised account recovery procedures.
- The bidder shall maintain documented endpoint isolation, containment, evidence preservation, and recovery procedures for ransomware, destructive malware, and misuse of administrative tools.
- The bidder shall provide monthly reporting on endpoint coverage, risk exposure, unresolved vulnerabilities, security incidents, and remediation activities

3.3 Network and Zero Trust Security

- The bidder shall design, implement, and maintain a Zero Trust Architecture across

Postbank's technology environment.

- The bidder shall implement network segmentation and micro-segmentation controls to protect critical banking systems, payment systems, privileged access zones, administrative environments, and third-party connectivity points.
- The bidder shall deploy and manage Network Detection and Response (NDR) capabilities integrated with intrusion prevention and threat intelligence platforms.
- The bidder shall continuously validate user identity, device posture, network trust, application access, and session risk before granting access to protected resources.
- The bidder shall implement controls to prevent lateral movement, privilege escalation, unauthorized access, and ransomware propagation across the network environment.
- The bidder shall provide real-time visibility into command-and-control communications, data exfiltration attempts, suspicious east-west traffic, and anomalous network behavior.

3.4 Identity and Authentication Security

- The bidder should implement and operate centralized Identity Governance and Administration (IGA) capabilities across all Postbank systems and platforms.
- The bidder shall enforce Multi-Factor Authentication (MFA) for all privileged, administrative, remote-access, cloud, and critical banking application accounts.
- The bidder shall implement Single Sign-On (SSO) capabilities wherever technically feasible and aligned with Postbank requirements.
- The bidder shall perform quarterly user access reviews and ensure segregation-of-duties controls are enforced across all critical systems.
- The bidder shall implement Identity Threat Detection and Response (ITDR) capabilities to identify and respond to suspicious authentication activity, privilege abuse, token theft, impossible-travel events, account compromise indicators, and MFA bypass attempts.
- The bidder shall maintain documented compromised-account recovery procedures covering credential resets, token revocation, session termination, privileged account validation, and restoration of trusted identity states.
- The bidder shall provide monthly access governance reports detailing user access privileges, role assignments, privileged accounts, and segregation-of-duties exceptions.

3.5 Privileged Access Management (PAM)

- The bidder shall implement, manage, and maintain a Privileged Access Management solution that protects all administrative, service, application, and privileged accounts.
- The bidder shall enforce least privilege principles, session monitoring, credential vaulting, automated password rotation, and privileged session recording.
- The bidder shall ensure all privileged activities are individually attributable, logged, monitored, and auditable.
- The bidder shall provide real-time alerting for suspicious privileged activities, unauthorized commands, unusual access behavior, and privilege escalation attempts.
- The bidder shall support immediate suspension, restriction, or revocation of privileged access during security incidents.
- The bidder shall maintain complete audit records to support investigations, compliance audits, and forensic activities.

3.6 Data Protection, Key Management and Compliance

- The bidder shall implement and maintain data protection controls aligned with PCI DSS, POPIA, ISO/IEC 27001, and other applicable regulatory requirements.
- The bidder shall deploy and manage Data Loss Prevention (DLP) controls across endpoints, email systems, cloud environments, and collaboration platforms.
- The bidder shall ensure sensitive information is encrypted in transit and at rest using industry-approved cryptographic standards.
- The bidder shall provide Hardware Security Module (HSM) services for secure generation, storage, protection, and management of cryptographic keys.
- The bidder should implement cyber recovery capabilities utilizing immutable, offline, logically isolated, or otherwise tamper-resistant backup technologies.
- The bidder shall conduct quarterly backup validation and recovery testing, including ransomware recovery scenarios and cyber resilience exercises.
- The bidder shall maintain documented cyber recovery architecture showing retention policies, recovery dependencies, restoration priorities, encryption controls, and segregation-of-duties requirements.

3.7 Incident Response, Recovery and Forensics

- The bidder shall develop, maintain, and operate a comprehensive Incident Response Plan that supports 24x7x365 incident detection, investigation, containment, eradication, recovery, and reporting.
- The bidder shall provide digital forensic investigation services, root cause analysis, evidence preservation, and breach assessment services.
- The bidder shall coordinate incident response activities with Postbank management, technical teams, legal representatives, auditors, and regulatory authorities as required.
- The bidder shall conduct quarterly incident simulation exercises and ransomware recovery testing.
- The bidder shall perform at least one annual end-to-end cyber recovery exercise involving critical banking services, identity systems, cloud services, endpoints, and infrastructure.
- The bidder shall provide structured evidence packs suitable for regulatory reporting, insurance claims, legal proceedings, and executive decision-making.

3.8 Threat Intelligence, Threat Hunting and Analytics

- The bidder shall integrate global, regional, and industry-specific threat intelligence feeds into the security monitoring environment.
- The bidder shall conduct proactive threat hunting activities on a continuous basis to identify advanced threats and previously undetected malicious activity.
- The bidder should provide weekly threat intelligence briefings and monthly strategic threat reports.
- The bidder should monitor emerging threats affecting the banking sector and provide recommendations to mitigate identified risks.

3.9 Cybersecurity Governance and Capacity Building

- The bidder shall develop and maintain an Information Security Operating Model aligned with SARB requirements, PCI DSS, and ISO/IEC 27001 standards.
- The bidder shall establish governance frameworks, reporting structures, policies, standards, procedures, and security metrics.
- The bidder shall conduct quarterly knowledge-transfer and mentorship sessions for

Postbank cybersecurity personnel.

- The bidder shall assist Postbank with cybersecurity workforce development, recruitment support, and skills enhancement initiatives.
- The bidder shall support the development and maintenance of executive cybersecurity dashboards and Board-level reporting.

3.10 Awareness and Insider Threat Management

- The bidder shall develop, implement, and maintain a comprehensive Cybersecurity Awareness and Insider Threat Management Programme aligned with Postbank's risk profile, regulatory obligations, and business objectives.
- The bidder shall conduct annual cybersecurity awareness training for all Postbank employees, contractors, consultants, and third-party users with access to Postbank systems and information assets.
- The bidder shall perform periodic phishing simulations, social engineering assessments, and targeted awareness campaigns to evaluate user behavior, measure security awareness maturity, and improve resilience against cyber threats.
- The bidder shall implement User and Entity Behavior Analytics (UEBA) capabilities to identify, monitor, and investigate abnormal user behavior, privileged user misuse, insider threats, account compromise indicators, and unauthorized access attempts.
- The bidder shall establish insider threat detection use cases covering data exfiltration, unusual access patterns, unauthorized privilege escalation, suspicious file transfers, anomalous working hours, and policy violations.
- The bidder shall provide quarterly reporting on cybersecurity awareness effectiveness, phishing simulation outcomes, insider threat investigations, user risk scores, and recommended improvement actions.
- The bidder shall develop and maintain measurable security culture metrics and maturity indicators to support continuous improvement and executive reporting.

3.11 Audit, Compliance and Risk Management

- The bidder shall support Postbank in maintaining a compliant and effective Information Security Management System (ISMS) aligned with ISO/IEC 27001, PCI
- DSS, PCI PIN Security Requirements, POPIA, SARB Cyber Resilience Guidance, and other applicable regulatory requirements.
- The bidder shall perform quarterly compliance assessments and control effectiveness reviews against applicable regulatory, legal, and contractual obligations.
- The bidder shall support annual PCI DSS certification, PCI PIN Security assessments, regulatory reviews, and independent security audits by providing evidence, technical support, and remediation guidance.
- The bidder shall maintain a comprehensive cybersecurity risk register identifying material risks, control deficiencies, compensating controls, remediation plans, ownership assignments, target remediation dates, and residual risks requiring formal acceptance by Postbank.
- The bidder shall provide cyber resilience evidence packs demonstrating control effectiveness, recovery assurance, threat scenario testing outcomes, incident response readiness, and third-party assurance activities.
- The bidder shall support internal audits, external audits, regulatory inspections, independent assessments, and assurance reviews by providing timely access to

documentation, evidence, and subject matter expertise.

- The bidder shall provide quarterly risk and compliance reports highlighting key risk indicators, compliance status, control maturity, emerging risks, remediation progress, and executive recommendations.

3.12 Security Device Management

- The bidder shall provide end-to-end management, administration, monitoring, maintenance, and optimization of Postbank security infrastructure.
- The bidder shall manage firewalls, intrusion prevention systems, web application firewalls, network security controls, email security gateways, endpoint protection platforms, secure web gateways, and any other security technologies designated by Postbank.
- The bidder shall perform continuous policy review, rule optimization, configuration management, performance monitoring, and security tuning to ensure optimal effectiveness of security controls.
- The bidder should ensure all security devices are maintained in accordance with vendor best practices and supported software versions.
- The bidder shall deploy security patches, firmware updates, and software upgrades in accordance with approved change management processes and defined service level agreements.
- The bidder shall manage and monitor all remote administration pathways, third-party access channels, emergency access procedures, and privileged administrative activities associated with managed security devices.
- The bidder shall ensure that all administrative access to security devices is protected through Privileged Access Management (PAM), Multi-Factor Authentication (MFA), comprehensive logging, and periodic access reviews.
- The bidder shall provide monthly operational reports detailing device health, security events, configuration changes, patch compliance status, access activities, and identified risks.

3.13 Email and Communication Security

- The bidder shall implement, manage, and maintain a secure email and communication security framework to protect Postbank against phishing, business email compromise, malware, spam, fraud, and other communication-based threats.
- The bidder shall deploy and operate secure email gateway technologies capable of advanced threat detection, attachment sandboxing, URL analysis, impersonation detection, and real-time threat prevention.
- The bidder shall implement and maintain Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) controls for all Postbank domains.
- The bidder shall provide advanced protection against business email compromise, account takeover, malicious forwarding rules, QR-code phishing, impersonation attacks, and abuse of collaboration platforms including Microsoft Teams, SharePoint, OneDrive, and Exchange Online.
- The bidder shall provide secure email archiving, journaling, retention management, legal hold capabilities, and e-discovery support in accordance with legal, regulatory, and business requirements.
- The bidder shall establish monitoring and response procedures for compromised

mailboxes, collaboration platforms, and communication systems, including evidence preservation, incident investigation, and rapid restoration of trusted access.

- The bidder shall provide monthly reporting on email security posture, phishing trends, malicious activity detected, incident response activities, and security improvement recommendations.

3.14 Patch and Vulnerability Management

- The bidder shall establish and operate a comprehensive Vulnerability and Patch Management Program covering all Postbank infrastructure, endpoints, applications, databases, cloud environments, network devices, and security platforms.
- The bidder shall conduct continuous vulnerability assessments and regular authenticated scanning activities across the Postbank environment.
- The bidder should prioritize vulnerabilities based on exploitability, business criticality, regulatory impact, exposure level, threat intelligence, and operational risk.
- The bidder shall ensure critical vulnerabilities are remediated within seven (7) calendar days unless otherwise approved through Postbank's formal risk acceptance process.
- The bidder shall conduct quarterly penetration testing and provide detailed reports, remediation recommendations, risk ratings, and validation testing outcomes.
- The bidder shall maintain a centralized vulnerability management repository containing identified vulnerabilities, remediation status, risk ratings, ownership assignments, compensating controls, and approved risk exceptions.
- The bidder shall distinguish and report on internet-facing vulnerabilities, identity-related vulnerabilities, ransomware-enabling vulnerabilities, critical banking service vulnerabilities, and cloud-related exposures.
- The bidder shall provide monthly executive and operational reporting detailing vulnerability trends, remediation performance, overdue findings, recurring root causes, risk acceptance items, and overall security posture.

3.15 Cloud and Application Security

- The bidder shall design, implement, operate, and continuously improve security controls across Postbank's cloud environments, applications, APIs, and digital service platforms.
- The bidder shall deploy and manage Cloud Security Posture Management (CSPM) capabilities to continuously monitor cloud configurations, identify security weaknesses, and enforce compliance requirements.
- The bidder shall implement cloud governance controls covering identity management, privileged access, workload protection, logging, monitoring, encryption, configuration management, and incident response.
- The bidder shall perform application security assessments utilizing Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software
- Composition Analysis (SCA), API security testing, and secure code review methodologies.
- The bidder shall establish secure software development and deployment controls aligned with DevOps principles and industry’s best practices.
- The bidder shall monitor, detect, and respond to Distributed Denial of Service (DDoS) attacks, application-layer attacks, API abuse, credential attacks, and other threats targeting internet-facing services.
- The bidder shall implement controls to identify exposed secrets, insecure configurations, vulnerable dependencies, unauthorized cloud resources, and application security

weaknesses.

- The bidder shall maintain secure configuration baselines for all cloud services, applications, APIs, containers, virtual machines, and supporting infrastructure.
- The bidder shall provide documented cloud compromise response procedures, recovery processes, forensic support capabilities, and restoration guidance for cloud-hosted services.
- The bidder shall provide monthly cloud and application security reports detailing security posture, identified vulnerabilities, threat activity, compliance status, remediation progress, and strategic recommendations for risk reduction.

4. Deliverables

4.1 Cybersecurity Deployment Roadmap (Post-Onboarding)

Phase	Timeline	Capable Area	Key deliverables	Objectives
Mandatory Security Tools Deployment	Month 1	Endpoint Security (EDR/XDR), Identity & Access, Email Security, Privileged Access	- Deploy Endpoint Security (EDR/XDR) - Deploy Multi-Factor Authentication (MFA) - Deploy Email Security Gateway / Protection - Deploy Privileged Access Management (PAM) - Integrate all tools with SOC monitoring and alert	Establish baseline security across endpoints, identities, privileged accounts, and email with full SOC visibility
SOC Platform Deployment (Parallel Implementation)	Months 1-2	SOC Core Platforms	- Deploy Security Information and Event Management (SIEM) - Deploy Security Orchestration, Automation and Response (SOAR) - Enable real-time log correlation and alerting - Achieve full SOC operational capability	Enable centralized monitoring, correlation, automation, and incident response capabilities
Threat Intelligence Capability	Within 3 Months	Threat Intelligence & Contextual Security	- Deploy Threat Intelligence Platform (TIP) - Integrate external and internal threat feeds - Implement IOC (Indicators of	Improve proactive threat detection and enhance SOC contextual awareness

			Compromise) management - Feed intelligence into SOC operations	
Full Cybersecurity Service Operationalization	Within 3 Months	End-to-End Cybersecurity Operations	- Continuous threat identification and monitoring - Incident detection, analysis, and response - Threat mitigation tracking and reporting - SOC dashboards for operational and executive reporting	Deliver a fully operational cybersecurity service with measurable detection, response, and governance reporting

4.2 Operations

- Fully deployed and configured PAM, endpoint security, email security, SOC, and MFA solutions.
- Comprehensive documentation: architecture diagrams, policies, and configuration guides.
- Regular vulnerability scanning and compliance reports.
- Incident reports and forensic investigation findings.
- End-of-contract migration plan, knowledge transfer, and handover documentation.
- Comprehensive Cybersecurity Maturity Assessment and 3-Year Roadmap.
- Quarterly Security Posture Report and KPI Dashboard.
- Annual Threat Intelligence Report for the Banking Sector.
- Annual Ransomware Readiness Report.
- Postbank-Specific Cyber Defense and Ransomware Protection Strategy.
- Cyber Recovery Architecture and Recovery Validation Report.
- Microsoft 365 / Office 365 Security Hardening and Recovery Report.
- Quarterly Identity Security and Privileged Access Assurance Report.
- Quarterly Crown-Jewel Protection and Segmentation Assurance Report.
- Annual Threat-Led Attack Simulation or Purple-Team Exercise Report were agreed by Postbank.
- Quarterly Audit and Compliance Review Reports.
- Knowledge Transfer and Capability Development Plan.

5. Service Delivery Requirements

5.1 Service Availability

- Provide 24x7x365 service coverage (including monitoring, support, and incident response).

5.2 Account Management

- Assign a dedicated Account Manager for Postbank engagement.
- Assign a dedicated Technical Lead responsible for service delivery and escalation management.

5.3 Hosting & Infrastructure Location

- All security and service delivery infrastructure (including SIEM, SOC, XDR, DLP, PAM, and related platforms) must be hosted within South Africa.

5.4 Data Sovereignty & Residency

- All logs, alerts, forensic artifacts, and security telemetry must remain fully resident within South African borders.
- No replication or storage of regulated data outside South Africa is permitted.

5.5 Insurance Requirement

- The service provider must maintain Professional Indemnity Insurance with a minimum coverage of R20 million.

5.6 Certifications & Skills Requirements

- The provider must be certified or formally partnered with at least three (3) of the following:
  - ISO 27001
  - PCI DSS QSA
  - CISSP
  - CEH
  - OSCP

6. Service Level Agreement (SLAs)

Service	KPI	Target
Incident detection to containment	Mean Time to Detect (MTTD)	Within 15 minutes
Response to critical incident	Mean Time to Respond (MTTR)	Within 30 minutes
Patch compliance	Endpoint/ server compliance	No less than 95% within 7 days particularly critical patches (within 7 days) and high-risk patches within 14 days
SOC up time and system availability	Availability	99.9% over 24/ 7
Recovery from ransomware simulation	Restore success	100%

Critical incident containment	Containment of confirmed critical cyber incident	Within 60 minutes unless otherwise agreed by incident commander and Postbank
Identity compromise response	Containment of confirmed compromised privileged account	Within 15 minutes of confirmed detection
Validated cyber recovery	Clean recovery of prioritised critical services	Within agreed service-specific recovery windows approved by Postbank
Critical asset log coverage	Critical agreed assets onboarded to SOC/ SIEM	Not less than 95%
Critical EDR/XDR coverage	Critical agreed servers/ endpoints covered	Not less than 95%
Overdue critical vulnerability rate	Critical vulnerabilities overdue beyond SLA	Not more than 5% without approved exception
Quarterly training	Attendance and competency	No less than 90%
Reporting	Operational reports	Monthly operational reports; quarterly executive dashboards.
Penetration Testing	Frequency	Conducted at least twice per year.

7. Compliance Requirements

The appointed service provider must ensure full alignment with, and where applicable, compliance with the following regulatory and industry frameworks:

7.1 Regulatory & Industry Compliance

The provider must demonstrate adherence to:

- South African Reserve Bank (SARB) Cybersecurity Directive
- Protection of Personal Information Act (POPIA)
- Payment Card Industry Data Security Standard (PCI DSS) (where applicable to payment environments)
- ISO/IEC 27001 Information Security Management Systems
- NIST Cybersecurity Framework (CSF)

7.2 Internal Governance Alignment

- The provider must align operational controls, reporting structures, and security processes with Postbank's internal risk management framework.
- All services must support regulatory audit readiness, evidence collection, and cyber resilience testing requirements as defined by Postbank.

7.3 Control Mapping & Evidence Requirements

- The bidder must provide comprehensive written control mappings demonstrating how proposed services, technologies, and processes align to each compliance requirement listed above.
- Evidence must be suitable for audit purposes and support ongoing compliance verification.

7.4 Regulatory Accountability

- The service provider will be responsible for execution, operational compliance, and advisory support.
- **Postbank retains ultimate accountability** for: Cybersecurity strategy
  - Risk acceptance decisions
  - Regulatory reporting obligations
- All formal submissions to regulatory and oversight bodies, including but not limited to: SARB
  - PASA
  - AGSA
  - POPIA Information Regulator

will be performed by Postbank.

8. Joint Controls and Transparency

To ensure effective governance, oversight, and regulatory assurance, the service provider must adhere to the following transparency and joint control requirements:

7.1 Data and Visibility Access

- The service provider must grant Postbank direct and real-time access to:
  - Raw security logs
  - Security dashboards
  - Vulnerability scan results
- Postbank must also have access to:
  - Security event and alert data
  - Case management and incident workflows
  - Detection content summaries (rules, logic, and tuning outputs)
  - Control coverage and effectiveness reports
  - Recovery and remediation evidence related to contracted services

8.2 Audit, Validation, and Independence Rights

- The service provider must not obstruct, restrict, or delay Postbank's ability to:
  - Perform independent validation of controls and outputs
  - Conduct audit reviews (internal or external)
  - Execute forensic investigations
  - Undertake transition or exit planning activities

8.3 Regulatory Reporting Support

- All formal regulatory submissions remain the responsibility of Postbank.
- The service provider must support these obligations by providing complete, accurate, and timely evidence packs, including audit-ready documentation.

8.4 Governance and Service Reviews

- The service provider must participate in quarterly service review meetings, chaired by Postbank.
- These reviews must cover service performance, risk posture, incidents, compliance status, and improvement actions.

8.5 Cyber Resilience Testing

- The service provider must support annual cyber resilience stress testing, aligned to SARB expectations and frameworks.
- Results, findings, and remediation actions must be fully documented and shared with Postbank.

9. Exit and Handover Requirements

The service provider must ensure a structured, fully supported, and risk-mitigated transition of services at the end of the contract period to prevent operational disruption and vendor lock-in.

9.1 Transition Support Obligations

- The service provider must provide comprehensive migration and exit support at the end of the three-year contract period.
- Transition activities must be executed in a manner that ensures continuous service availability and operational stability throughout the handover process.

9.2 Transition Planning Timeline

- Within the first six (6) months of contract commencement, the service provider must submit a documented transition-out plan.
- This plan must be maintained and updated throughout the contract lifecycle to reflect changes in architecture, tooling, and operating models.

9.3 Knowledge Transfer and Operational Independence

- At least six (6) months prior to contract expiry, the service provider must initiate a formal handover program covering:
  - Tooling configuration and administration
  - Operational playbooks and procedures
  - Security credentials and access governance structures
- Postbank must be enabled to operate all critical security controls independently, without reliance on the outgoing service provider.

9.4 Documentation and Deliverables

The service provider must deliver complete and current documentation, including:
System configurations

- Operational procedures and runbooks
- Detection rules, tuning logic, and use-case libraries
- Architecture diagrams and integration mappings
- Incident response and recovery playbooks

9.5 Training and Capability Uplift

- The service provider must conduct structured knowledge transfer and training sessions for Postbank internal teams.
- In addition, the provider must deliver quarterly capability uplift workshops to ensure ongoing skills development and operational readiness.

9.6 Tooling Portability and Exit Assurance

- The transition must be executed in a manner that ensures no vendor locks in.
- All tooling, configurations, detection content, workflows, and service data must be:
  - Fully exportable
  - Usable in standard or transferable formats
  - Free from restrictive licensing or undisclosed technical dependencies that impede migration

9.7 Transition Outcome Requirement

- The final objective of the exit process is to ensure a seamless operational handover, enabling Postbank or its nominated successor provider to assume full operational responsibility without degradation of security posture or service continuity.

10. Special Conditions of the Contract

The following special conditions shall apply to the appointed service provider throughout the duration of the contract:

10.1 Integrated Operating Model

- The bidder must deliver integrated security operations services in close collaboration with Postbank personnel.
- The operating model must enable joint execution of security functions, ensuring effective knowledge sharing, operational alignment, and shared accountability where applicable.

10.2 Personnel Vetting Requirements

- All personnel assigned to the Postbank environment must be subject to:
  - ITC (credit) clearance
  - Criminal background clearance
- Evidence of clearance must be made available to Postbank upon request and prior to onboarding of any personnel

10.3 Operational Readiness and Exercise Participation

- The successful bidder must actively participate in:
  - Scenario-based service reviews
  - Tabletop exercises
  - Cyber incident simulation and recovery exercises
- These activities will be scheduled and directed by Postbank as part of ongoing cyber resilience validation.

10.4 Incident Management and Executive Support

- The successful bidder must provide full support to Postbank during:
  - Major incident management and response activities
  - Executive-level reporting and briefings
  - Internal and external audit engagements

- Regulatory evidence preparation related to the contracted services
- Support must be provided in a timely, structured, and audit-ready manner, aligned to Postbank's governance and regulatory obligations.

11. Bid Evaluation Criteria and Process

The bid will be evaluated as follows:

- **Phase 1: Mandatory Requirements Criteria -** Only bidders that have complied with the mandatory criteria will be evaluated for functionality**.**
- **Phase 2: Functionality Requirements Criteria -** Bidders will be assessed on their capability to provide the service. Only bidders who have scored 70 points or more out of 100 on functionality will be further evaluated**.**
- **Phase 3: Live Demo** – Bidders must meet all requirements to be evaluated on price and specific goals
- **Phase 4: Commercial -** Price and Specific Goals (80/20 or 90/10)

11.1 Phase 1: Mandatory Requirements Criteria

No.	Mandatory Requirements	Comply	Do Not Comply
11.1.1	**Confirmation Letter** The bidder must submit a signed confirmation letter on official company letterhead confirming that: The bidder will fully comply with all specifications outlined in this tender document; and The bidder has the capacity, capability, and resources to deliver the required services in accordance with the stated specifications.		
11.1.2	**Team Credentials** The bidder must provide a minimum of two (2) suitably qualified and certified resources, as follows: • One (1) resource certified as CISO (Certified Information Security Officer); and • One (1) resource certified as CISSP (Certified Information Systems Security Professional). The bidder must include: • Detailed CVs of nominated resources • Valid copies of professional certifications • Evidence of relevant experience in cybersecurity or SOC environments		
11.1.3	**Local Presence:** The bidder must demonstrate the ability to deliver services within South Africa and maintain a permanent operational presence in-		

	country, including local support capability. The bidder must provide: • Physical office address in South Africa (preferably Pretoria or Johannesburg) • Proof of premises, such as: o Municipal account/utility bill; and/or Lease agreement or title deed confirming occupancy or ownership of premises		

11.1.4	**Technical Response Document:**
	
	The bidder must submit a comprehensive Technical Response Document covering, at minimum, the following areas:
	• Proposed approach and delivery methodology
	• Capacity and skills transfer plan
	• SOC architecture, infrastructure, and security toolset capabilities
	• Postbank-specific cyber defense and ransomware protection strategy
	• Cyber recovery, backup, and restoration approach
	• Microsoft 365 / Office 365 security and protection strategy
	• Identity and privileged access management strategy
	• Protection approach for:
	  o Core banking systems
	  o Payment and card processing environments
	  o ATM networks
	  o Critical third-party and vendor access
	• Transition approach including:
	  o Transition-in plan
	  o State-state operating model
	  o Transition-out and exit strategy		

11.1.5	**Cyber Defence and Ransomware Strategy** The bidder must submit a Postbank-specific Cyber Defense and Ransomware Protection Strategy addressing the full lifecycle of cyber operations, including: • Prevention • Detection • Containment • Eradication • Recovery • Recovery validation • Executive reporting and regulatory support		
11.1.6	**Banking Sector Experience** The bidder must demonstrate that it has delivered cybersecurity managed services within the last three years to at least one of the		

	following: • A regulated financial institution, such as a bank, payment institution, insurer, or other regulated financial services organization; or • An organization of equivalent size, complexity and criticality, where the cybersecurity environment has comparable requirements to a bank. Evidence must include details of current and/or recent engagements, including scope and relevance to services required under this tender.		
11.1.7	**Recovery Assurance Capability** The bidder must provide evidence of capability to support: • Immutable or tamper-resistant backup and recovery solutions • Recovery validation processes and assurance testing • Participation in cyber recovery exercises and scenario simulations • End-to-end recovery assurance aligned to business continuity and regulatory requirements		

11.2 Phase 2: Functional Requirements Criteria

A total of 200 points is allocated for functional requirements. Bidders will be assessed on their capability to provide the service. Only bidders that have scored 70 points for Part A and 70 points for Part B will proceed to the next stage**.**

Part A

Item No.	Criteria	Sub-Criteria	Weight
11.2.1	**Company Experience** The bidder must have a minimum of five (5) years of experience in implementing IT security services, managing the infrastructure, and providing support and maintenance The bidder must provide as proof a company profile indicating experience, covering the following: • Number of years the firm has been in existence. • Detailed list of services offered by the company (Cybersecurity) • List of support staff and their roles	• Company Profile with ≥5 years' experience delivery of similar projects (implementing IT security services, managing the infrastructure, and providing support and maintenance = **25 points** • Company Profile with <5 years' experience delivery of similar projects (implementing IT security services, managing the infrastructure, and providing support and maintenance) = **0 Points**	**25**

	relevant to the service		
11.2.2	**Company Track record** The bidder must have provided IT Security services to various clients within the financial services sector over the past five years or related industries. The bidder must provide a minimum of three signed reference letters detailing the successful completion of the service (s). Providing more information will be to the bidder's advantage (Signed Reference letters on client letterheads must be attached). The reference letters must include the following: • Company Name • Company Contact details and address • Contact Person • Description of services rendered • Period/ Duration of the Project (include start and end date)	• No reference letter attached or less than three (3) reference letters attached = **0 points.** • 3≤5 Reference letters with required information where similar projects were (IT security services and maintenance were rendered in the past five (5) years = **15 points** • >5 Reference letters with required information where similar projects were (in the past five (5) years = **25 points**	**25**
11.2.3	**Project resources** The bidder must provide a detailed profile of the Project Lead who will work on the Postbank Account. The Project Team Lead must have the skills and experience implementing IT security projects and should have no less than five (5) years of relevant experience related to this project. The bidder must provide a Project Lead CV indicating the skills and years of experience implementing the IT security project.	• Project lead CV with <5 years of experience in IT security services = **0 points** • Project Lead CV with 5 <7 years of experience in IT security implementation = **15 points** • Project Lead CV with >7 years of experience in IT security = **25 points**	**25**
11.2.4	**Regulatory Compliance and Certifications** The bidder must be able to produce the compliance report for **PCI DSS**: The bidder must provide an up-to-date Report of Compliance (ROC) **ISO27001:** Certificate (from an accredited	Three reports = **25 points** Two reports =**15 points** No report = **0 points**	**25**

	certification body) or Latest audit report And **POPIA**: Bidder must provide a compliance report instead		
Total			**100 Points**

Part B

Item No.	Criteria	Sub-Criteria	Weight
11.2.5	**Cyber Defense and Ransomware Protection Strategy** Postbank-specific written strategy and operating model	• **0–5 Points**: Weak or generic response with minimal relevance to Postbank and limited practical implementation details. • **6–15 Points:** Relevant response that addresses key areas but lacks completeness, integration, or operational detail. • **16–25 Points:** Comprehensive, practical, and Postbank-specific strategy with clear governance, operational processes, detection and response capabilities, and recovery measures.	**25**
11.2.6	**Recovery and Cyber Resilience Capability** Recovery design, clean recovery, validation, exercise evidence	• **0–5 Points**: Weak or generic response with minimal relevance to Postbank and limited practical implementation details. • **6–15 Points**: Relevant response that addresses key areas but lacks completeness, integration, or operational detail. • **16–25 Points**: Comprehensive, practical, and Postbank-specific strategy with clear governance, operational processes, detection and response capabilities, and recovery measures.	**25**

11.2.7	**SOC and Incident Response Operating Maturity** Analyst model, playbooks, detection engineering, case management, transparency, reporting	• **0–5 Points**: Weak or generic response with minimal relevance to Postbank and limited practical implementation details. • **6–15 Points**: Relevant response that addresses key areas but lacks completeness, integration, or operational detail. • **16–25 Points:** Comprehensive, practical, and Postbank-specific strategy with clear governance, operational processes, detection and response capabilities, and recovery measures.	**25**
11.2.8	**Financial Sector Delivery Depth** Evidence of delivering to regulated banking/financial clients of similar criticality	• **0–5 Points**: Weak or generic response with minimal relevance to Postbank and limited practical implementation details. • **6–15 Points**: Relevant response that addresses key areas but lacks completeness, integration, or operational detail. • **16–25 Points**: Comprehensive, practical, and Postbank-specific strategy with clear governance, operational processes, detection and response capabilities, and recovery measures.	**25**
Total			**100 Points**

11.3 Phase 3: Live Demonstration

Item No,	Demo Requirements	Yes/No
11.3.1	**SOC Visibility and Data Ingestion** 24/7 monitoring logs, alerts, and incidents. Incident response and forensic investigation capabilities.	
11.3.2	**SIEM Capability and Search Performance**: Integration with SIEM and threat intelligence feeds	

11.3.3	**Threat Detection and Correlation Rules**: Detect unusual behaviour compared to the normal baseline	
11.3.4	**Incident Response Lifecycle**: Establish and maintain the Incident Response Plan (IRP)	
11.3.5	**SOA (Security Orchestration Automation and Response** Integrating multiple security technologies and workflows	
11.3.6	**EDR/XDR Capability** Isolate endpoint, kill processes, quarantine files, restrict user sessions.	
11.3.7	**Dashboarding and Reporting** Active incidents, severity levels, detection trends.	
11.3.8	**SOC Team Structure and Skills** • Level 1 skills • Level 2 skills and capability	
11.3.9	**Threat Hunting and Capability** Identify early-stage attacks, stealthy adversaries, and advanced persistent threats (APT)	
11.3.10	**Compliance and Governance** Ensure SOC operations adhere to applicable laws, regulations, and standards.	
11.3.11	**Operational Maturity evaluation (SOC Maturity Model)** • People and skills • Process and Procedure	
11.3.12	**Ransomware Attack Scenario Demonstration** – The bidder must demonstrate how the SOC and response capability would detect, contain, investigate, and support recovery for a ransomware attack affecting endpoints, privileged accounts, and critical services.	
11.3.13	**Microsoft 365 / Office 365 Compromise Scenario** – The bidder must demonstrate how a mailbox compromise, suspicious forwarding rule, Open Authorisation abuse, or business email compromise event would be detected, contained, and recovered.	
11.3.14	**Recovery Validation Scenario** – The bidder must demonstrate how restored services would be validated as clean and trustworthy before return to production use.	

11.4 Independent Verification

The bidder acknowledges and agrees that Postbank retains the right to independently verify service quality, performance, and compliance at any time during the contract period.

The bidder shall facilitate reference checks by Postbank, including engagement with current or previous clients of the bidder, where reasonably required to validate capability, service performance, and delivery track record.
The bidder shall support and cooperate with annual independent audits of all Security Operations Centre (SOC), Extended Detection and Response (XDR), and associated managed security services provided under this contract.
Such independent audits may assess operational effectiveness, control maturity, security architecture alignment, incident response capability, compliance with contractual obligations, and adherence to applicable standards including PCI DSS, ISO/IEC 27001, POPIA, and SARB cyber resilience expectations.
The bidder shall ensure that audit findings, recommendations, and remediation actions are formally documented, tracked, and addressed within agreed timelines.
The bidder shall provide full cooperation during audits and shall supply all required evidence, system access (subject to security controls), documentation, and personnel support necessary for audit execution.
Audit results, including executive summaries and material findings, shall be shared with Postbank and, where required, relevant regulatory authorities.

11.5 Phase 4: Commercial - Price and Specific Goals (80/20 or 90/10)

Only bidders that have satisfied all mandatory requirements, achieved the minimum functionality threshold, and successfully demonstrated the required operational capabilities in the live demonstration stage shall proceed to price and specific goals evaluation.

The evaluation for Price and Specific Goals shall be based on the PPPFA principle, and the points for evaluation criteria are as follows:

EVALUATION CRITERIA		POINTS
11.5.1	**PRICE**	**90**
11.5.2	**SPECIFIC GOALS**	**10**
Total		**100**

SECTION 5
PRICING SCHEDULE/COSTING MODEL

1The service provider/supplier is required to provide a full cost breakdown for each item required on an official company letterhead.

2The service provider/supplier is required to list all additional costs associated with the services listed above, with the conditions of when such costs will apply.

3All prices must be VAT inclusive (if VAT registered) and must be quoted in South African Rand (ZAR);

Description	Quantity	Once-off Cost	Year 1	Year 2	Year 3
Project Initiation and Mobilization					
Implementation and Deployment Services					
SOC Onboarding and Integration					
Knowledge Transfer and Training					
Transition-In Services					
24x7 SOC Monitoring Services					
Managed Services					
SIEM Licensing					
SOAR Licensing					
EDR/XDR Licensing					
PAM Licensing					
DLP Licensing					
Cloud Hosting Costs					
Other Operational Services Costs (Clearly explain the costs)					
Total (Excluding VAT)					
VAT (15%)					
Total (Including VAT)					

The service provider warrants that the pricing quoted above is in line with the Specification and is free of any errors and omissions and that he/she is able to deliver the service on the quoted price.

NAME OF DELEGATED SIGNATORY: .....……..

(PRINT) in his capacity of

DESIGNATION OF SIGNATORY: .....

(PRINT) who warrants his authority to sign on behalf of

SIGNATURE:.....

NAME OF BIDDER (COMPANY) : .....

DATE: .....……

DECLARATION

I, _____, hereby declare that the information provided above is correct and

that there is no misrepresentation of facts.

SBD 4

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. Bidder's declaration

2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest1 in the enterprise, employed by the state? **YES/NO**

2.1.1 If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below.

Full Name	Identity Number	Name of State institution

2.2 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution? **YES/NO**

SBD 4

2.2.1 If so, furnish particulars:

1 the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise

……
……

2.3 Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract? **YES/NO**

2.3.1 If so, furnish particulars:
……..
……..

3 DECLARATION

I, the undersigned, (name)…… in submitting the accompanying bid, do hereby make the following statements that I certify to be true and complete in every respect:

3.1 I have read and I understand the contents of this disclosure;
3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;
3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium2 will not be construed as collusive bidding.
3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.
3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.

3.5 There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.

3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and

Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

---

[2] Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT.

I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

…… ……
Signature Date

…… ……
Position Name of bidder

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to tender:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 **To be completed by the organ of state**

a) The applicable preference point system for this tender is the 80/20 or 90/10 preference point system.

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:
(a) Price; and
(b) Specific Goals.

1.4 **To be completed by the organ of state:**

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	90
SPECIFIC GOALS	10
Total points for Price and SPECIFIC GOALS	**100**

1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.

1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

(a) **"tender"** means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;
(b) **"price"** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;

(c) **"rand value"** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;

(d) **"tender for income-generating contracts"** means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and

(e) **"the Act"** means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULA FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20or90/10

$$\boldsymbol{Ps = 80\left(1 - \frac{Pt - P\,min}{P\,min}\right)} \text{or} \boldsymbol{Ps = 90\left(1 - \frac{Pt - P\,min}{P\,min}\right)}$$

Where
Ps=Points scored for price of tender under consideration
Pt=Price of tender under consideration
Pmin=Price of lowest acceptable tender

3.2. FORMULA FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT

3.2.1. POINTS AWARDED FOR PRICE

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20 or 90/10

$$\boldsymbol{Ps = 80\left(1 + \frac{Pt - P\,max}{P\,max}\right)} \text{or} \boldsymbol{Ps = 90\left(1 + \frac{Pt - P\,max}{Pmax}\right)}$$

Where
Ps=Points scored for price of tender under consideration
Pt=Price of tender under consideration
Pmax=Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:

4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point

system applies, an organ of state must, in the tender documents, stipulate in the case of—

(a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or

(b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,

then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.
(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.
***Note to tenderers: The tenderer must indicate how they claim points for each preference point system.*)**

The specific goals allocated points in terms of this tender	Number of points allocated (90/10 system) (To be completed by the organ of state)	Number of points claimed (90/10 system) (To be completed by the tenderer)
Historically Disadvantaged individuals (51% and above)	**5**	
Women (51% and above)	**3**	
Disabled (51% and above)	**2**	

DECLARATION WITH REGARD TO COMPANY/FIRM

4.3. Name of company/firm: ……
4.4. Company registration number: …….
4.5. TYPE OF COMPANY/ FIRM

- ☐ Partnership/Joint Venture / Consortium
- ☐ One-person business/sole propriety
- ☐ Close corporation
- ☐ Public Company
- ☐ Personal Liability Company
- ☐ (Pty) Limited
- ☐ Non-Profit Company
- ☐ State Owned Company

[Tick applicable box]

4.6. I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:

i) The information furnished is true and correct;
ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;

iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;
iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –

(a) disqualify the person from the tendering process;
(b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
(c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
(d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
(e) forward the matter for criminal prosecution, if deemed necessary.

.....
SIGNATURE(S) OF TENDERER(S)

SURNAME AND NAME: .....
DATE:.....

ADDRESS:.....

.....

.....
.....

SECTION 7

GOVERNMENT PROCUREMENT: GENERAL CONDITIONS OF CONTRACT – JULY 2011

NOTES

The purpose of this document is to:

(i) Draw special attention to certain general conditions applicable to government Bids, contracts and orders; and

(ii) To ensure that clients be familiar with regard to the rights and obligations of all parties involved in doing business with government.

In this document words in the singular also mean in the plural and vice versa and words in the masculine also mean in the feminine and neuter.

 The GCC will form part of all bid documents and may not be amended.

 Special Conditions of Contract (SCC) relevant to a specific bid, should be compiled separately for every bid (if (applicable) and will supplement the GCC. Whenever there is a conflict, the provisions in the SCC shall prevail.

TABLE OF CLAUSES

1. Definitions
2. Application
3. General
4. Standards
5. Use of contract documents and information; inspection
6. Patent rights
7. Performance security
8. Inspections, tests and analysis
9. Packing
10. Delivery and documents
11. Insurance
12. Transportation
13. Incidental services
14. Spare parts
15. Warranty
16. Payment

17. Prices
18. Contract amendments
19. Assignment
20. Subcontracts
21. Delays in the supplier's performance
22. Penalties
23. Termination for default
24. Dumping and countervailing duties
25. Force Majeure
26. Termination for insolvency
27. Settlement of disputes
28. Limitation of liability
29. Governing language
30. Applicable law
31. Notices
32. Taxes and duties
33. National Industrial Participation Programme (NIPP)
34. Prohibition of restrictive practices

General conditions of contract

1. Definitions

1 The following terms shall be interpreted as indicated:

1.1 "Closing time" means the date and hour specified in the bidding documents for the receipt of Bids.

1.2 "Contract" means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

1.3 "Contract price" means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.

1.4 "Corrupt practice" means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

1.5 "Countervailing duties" are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally.

1.6 "Country of origin" means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing,

processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.

1.7 “Day” means calendar day.

1.8 “Delivery” means delivery in compliance of the conditions of the contract or order.

1.9 “Delivery ex stock” means immediate delivery directly from stock actually on hand.

1.10 “Delivery into consignees store or to his site” means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.

1.11 "Dumping" occurs when a private enterprise abroad market its goods on own initiative in the RSA at lower prices than that of the country of origin and which have the potential to harm the local industries in the RSA.

1.12 “Force majeure” means an event beyond the control of the supplier and not involving the supplier’s fault or negligence and not foreseeable. Such events may include, but is not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

1.13 “Fraudulent practice” means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the bidder of the benefits of free and open competition.

1.14 “GCC” means the General Conditions of Contract.

1.15 “Goods” means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.

1.16 “Imported content” means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the supplies covered by the bid will be manufactured.

1.17 “Local content” means that portion of the bidding price which is not included in the imported content provided that local manufacture does take place.

1.18 “Manufacture” means the production of products in a factory using labour, materials, components and machinery and includes other related value-adding activities.

1.19 “Order” means an official written order issued for the supply of goods or works or the

rendering of a service.

1.20 “Project site,” where applicable, means the place indicated in bidding documents.

1.21 “Purchaser” means the organisation purchasing the goods.

1.22 “Republic” means the RSA.

1.23 “SCC” means the Special Conditions of Contract.

1.24 “Services” means those functional services ancillary to the supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance and other such obligations of the supplier covered under the contract.

1.25 “Written” or “in writing” means handwritten in ink or any form of electronic or mechanical writing.

2 Application

2.1 These general conditions are applicable to all Bids, contracts and orders including Bids for functional and professional services, sales, hiring, letting and the granting or acquiring of rights, but excluding immovable property, unless otherwise indicated in the bidding documents.

2.2 Where applicable, SCC are also laid down to cover specific supplies, services or works.

2.3 Where such SCC are in conflict with these general conditions, the special conditions shall apply.

3 General

3.1 Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid. Where applicable a non-refundable fee for documents may be charged.

3.2 With certain exceptions, invitations to bid are only published in the Government Tender Bulletin. The Government Tender Bulletin may be obtained directly from the Government Printer, Private Bag X85, Pretoria 0001, or accessed electronically from www.treasury.gov.za

4 Standards

4.1 The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.

1 Use of contract documents and information; inspection

5.1 The supplier shall not, without the purchaser’s prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or

information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

5.2 The supplier shall not, without the purchaser's prior written consent, make use of any document or information mentioned in GCC clause 5.1 except for purposes of performing the contract.

5.3 Any document, other than the contract itself mentioned in GCC clause 5.1 shall remain the property of the purchaser and shall be returned (all copies) to the purchaser on completion of the supplier's performance under the contract if so required by the purchaser.

5.4 The supplier shall permit the purchaser to inspect the supplier's records relating to the performance of the supplier and to have them audited by auditors appointed by the purchaser, if so required by the purchaser.

6 Patent rights

6.1 The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the goods or any part thereof by the purchaser.

7 Performance security

7.1 Within thirty (30) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in SCC.

7.2 The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.

7.3 The performance security shall be denominated in the currency of the contract, or in a freely convertible currency acceptable to the purchaser and shall be in one of the following forms:

7.3.1 a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in the purchaser's country or abroad, acceptable to the purchaser, in the form provided in the bidding documents or another form acceptable to the purchaser; or

7.3.2 a cashier's or certified cheque

7.4 The performance security will be discharged by the purchaser and returned to the supplier not later than thirty (30) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless

otherwise specified in SCC.

8. Inspections, tests and analyses

8.1 All pre-bidding testing will be for the account of the bidder.

8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the Department or an organisation acting on behalf of the Department.

8.3 If there are no inspection requirements indicated in the bidding documents and no mention is made in the contract, but during the contract period it is decided that inspections shall be carried out, the purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.

8.4 If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the supplies to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.

8.5 Where the supplies or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such supplies or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.

8.6 Supplies and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected.

8.7 Any contract supplies may on or after delivery be inspected, tested or analyzed and may be rejected if found not to comply with the requirements of the contract. Such rejected supplies shall be held at the cost and risk of the supplier who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with supplies which do comply with the requirements of the contract. Failing such removal the rejected supplies shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute supplies forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected supplies, purchase such supplies as may be necessary at the expense of the supplier.

8.8 The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 23 of GCC.

9 Packing

9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract, including additional requirements, if any, specified in SCC, and in any subsequent instructions ordered by the purchaser.

10 Delivery and documents

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified in SCC.

10.2 Documents to be submitted by the supplier are specified in SCC.

11 Insurance

11.1 The goods supplied under the contract shall be fully insured in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery in the manner specified in the SCC.

12 Transportation

12.1 Should a price other than an all-inclusive delivered price be required, this shall be specified in the SCC.

13 Incidental services

13.1 The supplier may be required to provide any or all of the following services, including additional services, if any, specified in SCC:

13.1.1 performance or supervision of on-site assembly and/or commissioning of the supplied goods;

13.1.2 furnishing of tools required for assembly and/or maintenance of the supplied goods;

13.1.3 furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;

13.1.4 performance or supervision or maintenance and/or repair of the supplied goods, for

a period of time agreed by the parties, provided that this service shall not relieve the supplier of any warranty obligations under this contract; and

13.1.5 training of the purchaser's personnel, at the supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied goods.

13.2 Prices charged by the supplier for incidental services, if not included in the contract price for the goods, shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the supplier for similar services.

14 Spare parts

14.1 As specified in SCC, the supplier may be required to provide any or all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier:

14.1.1 such spare parts as the purchaser may elect to purchase from the supplier, provided that this election shall not relieve the supplier of any warranty obligations under the contract; and

14.1.2 in the event of termination of production of the spare parts:

14.1.2.1 Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and

14.1.2.2 following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15 Warranty

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications) or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.2 This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in SCC.

15.3 The purchaser shall promptly notify the supplier in writing of any claims arising under this

warranty.

15.4 Upon receipt of such notice, the supplier shall, within the period specified in SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.5 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in SCC, the purchaser may proceed to take such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16 Payment

16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in SCC.

16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfilment of other obligations stipulated in the contract.

16.3 Payments shall be made promptly by the purchaser, but in no case later than thirty (30) days after submission of an invoice or claim by the supplier.

16.4 Payment will be made in rand unless otherwise stipulated in SCC.

17 Prices

17.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in his bid, with the exception of any price adjustments authorised in SCC or in the purchaser's request for bid validity extension, as the case may be.

18 Contract amendments

18.1 No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties concerned.

19 Assignment

19.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the purchaser's prior written consent.

20 Subcontracts

20.1 The supplier shall notify the purchaser in writing of all subcontracts awarded under this contract if not already specified in the bid. Such notification, in the original bid or later, shall not relieve the supplier from any liability or obligation under the contract.

21 **Delays in the supplier's performance**

21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.

21.2 If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.

21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.

21.4 The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.

21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 21.2 without the application of penalties.

21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without cancelling the contract, be entitled to purchase supplies of a similar quality and up to the same quantity in substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and without prejudice to his other rights, be entitled to claim damages from the supplier.

22 Penalties

22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services using the current prime interest rate calculated for each day of the delay until actual delivery or performance. The purchaser may also consider termination of the

contract pursuant to GCC Clause 23.

23 Termination for default

23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:

23.1.1 if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;

23.1.2 if the Supplier fails to perform any other obligation(s) under the contract; or

23.1.3 if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

23.2 In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.

23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.

23.4 If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than fourteen (14) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated fourteen (14) days the purchaser may regard the intended penalty as not objected against and may impose it on the supplier.

23.5 Any restriction imposed on any person by the Accounting Officer / Authority will, at the discretion of the Accounting Officer / Authority, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person, is or was in the opinion of the Accounting Officer / Authority actively associated.

23.6 If a restriction is imposed, the purchaser must, within five (5) working days of such imposition, furnish the National Treasury, with the following information:

23.6.1 the name and address of the supplier and / or person restricted by the purchaser;

23.6.2 the date of commencement of the restriction

23.6.3 the period of restriction; and

23.6.4 the reasons for the restriction.

23.7 These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.8 If a court of law convicts a person of an offence as contemplated in sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.

24 Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or anti-dumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidized import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall on demand be paid forthwith by the contractor to the State or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which may be due to him.

25 *Force majeure*

25.1 Notwithstanding the provisions of GCC Clauses 22 and 23, the supplier shall not be liable for forfeiture of its performance security, damages, or termination for default if and to the extent that his delay in performance or other failure to perform his obligations under the contract is the result of an event of force majeure.

25.2 If a force majeure situation arises, the supplier shall promptly notify the purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical, and shall seek all reasonable alternative means

for performance not prevented by the force majeure event.

26 Termination for insolvency

26.1 The purchaser may at any time terminate the contract by giving written notice to the supplier if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

27 Settlement of disputes

27.1 If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

27.2 If, after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

27.3 Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.

27.4 Mediation proceedings shall be conducted in accordance with the rules of procedure specified in the SCC.

27.5 Notwithstanding any reference to mediation and/or court proceedings herein,

27.5.1 the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and

27.5.2 the purchaser shall pay the supplier any monies due the supplier.

28 Limitation of liability

28.1 Except in cases of criminal negligence or wilful misconduct, and in the case of infringement pursuant to Clause 6;

28.1.1 the supplier shall not be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser; and

28.1.2 the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the total contract price, provided that this

limitation shall not apply to the cost of repairing or replacing defective equipment.

29 Governing language

29.1 The contract shall be written in English. All correspondence and other documents pertaining to the contract that is exchanged by the parties shall also be written in English.

30 Applicable law

30.1 The contract shall be interpreted in accordance with South African laws, unless otherwise specified in SCC.

31 Notices

31.1 Every written acceptance of a bid shall be posted to the supplier concerned by registered or certified mail and any other notice to him shall be posted by ordinary mail to the address furnished in his bid or to the address notified later by him in writing and such posting shall be deemed to be proper service of such notice

31.2 The time mentioned in the contract documents for performing any act after such aforesaid notice has been given, shall be reckoned from the date of posting of such notice.

32 Taxes and duties

32.1 A foreign supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the purchaser's country.

32.2 A local supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted goods to the purchaser.

32.3 No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid the Department must be in possession of a tax clearance certificate, submitted by the bidder. This certificate must be an original issued by the SARSs.

33 National Industrial Participation (NIP) Programme

33.1 The NIP Programme administered by the DTI shall be applicable to all contracts that are subject to the NIP obligation.

34 Prohibition of restrictive practices

34.1 In terms of section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, an agreement between, or concerted practice by, firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder (s) is / are or a contractor(s) was / were involved in collusive bidding (or bid rigging).

34.2 If a bidder(s) or contractor(s), based on reasonable grounds or evidence obtained by the purchaser, has / have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in the Competition Act No. 89 of 1998.

34.3 If a bidder(s) or contractor(s), has / have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and / or terminate the contract in whole or part, and / or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding ten (10) years and / or claim damages from the bidder(s) or contractor(s) concerned

The above General Conditions of Contract (GCC) are accepted by:

Name:	
Designation:	
Bidder:	
Signature:	
Date:	