BID NO:009-2025/2026

APPOINTMENT OF A SERVICE PROVIDER FOR FULL TURN-KEY MANAGED INFORMATION AND COMMUNICATION SERVICES(ICT) FOR THE CETA FOR THREE (3) YEARS.

RFP NUMBER:	**BID NO: 009-2025/2026**
DESCRIPTION:	**APPOINTMENT OF A SERVICE PROVIDER FOR FULL TURN-KEY MANAGED INFORMATION AND COMMUNICATION SERVICES (ICT) FOR THE CETA FOR THREE (3) YEARS**
ADVERT / PUBLISH DATE:	**09 December 2025**
CLOSING DATE:	**27 January 2026**
CLOSING TIME:	**11h00**
VALIDITY PERIOD	**90 days from the closing date**
PREFERENCE POINT SYSTEM	**80/20**
BRIEFING SESSION	**Compulsory attendance 09 January 2026 09:00am – 09:50am.** **CETA Head Office** **52 14th Road** **Noordwyk** **Midrand** **1687**
BID RESPONSES MUST BE HAND DELIVERED TO:	**CETA Head Office** **52 14th Road** **Noordwyk** **Midrand** **1687**
ATTENTION:	**Supply Chain Management – Bids**

NB: Bidders must ensure that they sign the tender register at the CETA Head Office Reception when delivering their bids responses. Bidders who will use Courier companies are to ensure that the Courier company writes the name of the bidding company on the tender register at CETA H/O Reception. Submissions not registered on the tender register will be disqualified. The closing time is as per the clock displayed at the CETA Head Office Reception.
The CETA reserves the right not to appoint or to cancel this tender at any time as circumstances dictates.
It should be noted that the award may not necessarily be to the lowest bidder; and that cost effectiveness does not equal the lowest price quote.

TERMS, ABBREVIATIONS AND ACRONYMS

Term	Description
ATR	Annual Training Report
CETA	Construction Education and Training Authority
DHET	Department of Higher Education and Training
DG	Discretionary grants
EFT	Electronic Funds Transfer
ETQA	Education and Training Quality Assurance
LMS	Learner Management System
NLRD	National Learner Records Database
NQF	National Qualification Framework
NSDP 2030	National Skills Development Plan 2030
OFO	Organized Framework for Occupations
QCTO	Quality Council for Trades and Occupations
SETIMS	Sector Education and Training Management Information System
SAQA	South African Qualification Authority
SDF	Skills Development Facilitator

SETA	Sector Education Training Authorities
SLA	Service Level Agreement
SDL	Skills Development Levy
WSP	Workplace Skills Plan

1.1. Criterion 1 – Mandatory Requirement: (Main Bidder)

Please note that failure to submit the following documents and/or proof will lead to immediate disqualification from bid evaluation process:

a. Bidders must have a valid Partnership Certificate **OR** Letter, **OR** Agreement with a South African telecommunications operator to meet the requirements of CETA.

b. A valid ISO 27001 certification for Information Security

c. A valid ISO 9001 certification for Quality Management

d. Relevant cloud platform certifications (Microsoft Azure preferred)

1.2. BID CONDITIONS

- All bidders are required to register on the National Treasury Central Supplier Database (CSD). The CSD proof of registration will be used by CETA to verify the bidder's tax and other compliant statuses. This RFP will only be awarded to bidders who are tax compliant on National Treasury CSD at the time of award.
- Proof of registration with the National Treasury Central Supplier Database (CSD).
- The CETA does not bind itself to accept or appoint any bidder or any RFP response, nor shall it be responsible for or pay any expenses or losses which may be incurred by the bidder in the preparation and delivery of the RFP.
- The recommended bidder will be subjected to a due diligence process prior to the appointment.
- CETA may require verifying and confirming the products to be supplied during the evaluation stage, and bidders to avail the premises and/or products on request. CETA will not be held liable for any expenses incurred during the evaluation stage or due diligence process.
- Joint Ventures (JV) – JVs are required to attach a signed JV agreement, attach CSD report of all JV members, attached completed and signed SBD4 documents of all JV members and a valid BBBEE certificate of the JV.

- No RFP shall be deemed to have been accepted unless and until a formal contract / letter of appointment is fully signed by parties and executed.
- CETA reserves the right to:
    a) Not evaluate and award RFP that do not comply strictly with the requirements of this RFP.
    b) Make a selection solely on the information received in the RFPs and enter into negotiations with any one or more of the preferred bidder(s) based on the criteria specified in this RFP.
    c) Contact any bidder during the evaluation process, in order to clarify any information, without informing any other bidders, and no change in the content of the RFP shall be sought, offered, or permitted.
    d) Withdraw the RFP at any stage and/or cancel this RFP or any part thereof at any stage as prescribed in the PPPFA regulations.
    e) Not award to the highest point scorer subject to the objective criteria as stipulated in the Preferential Procurement Policy.

SBD DOCUMENTS

Please note that the following documents must be completed and signed.

- SBD 1,
- SBD 4,
- SBD 6.1,
- SBD 7.2, and
- GCC.

OTHER REQUIRED DOCUMENTS

Please note that failure to attach the following documents will result in the forfeiture of preference points:

1. **EMEs:** Sworn affidavit confirming their annual total revenue of R10 million or less and level of black ownership or a B-BBEE level verification certificate.
2. **QSEs:** Sworn affidavit confirming their annual total revenue of between R10 million and R50 million and level of black ownership or B-BBEE level verification certificate.
3. **Bidders other than EMEs and QSEs:** Original and valid B-BBEE status level verification certificate verified by a SANAS accredited verification agency, or a certified copy thereof.

Bidders must submit proof of documentation required in terms of this RFP to claim points for specific goals

Please double-check that you have attached all the above documents before submitting your bid document.

BID DOCUMENTS CHECK LIST:

The contents of the RFP document must be as follows, and numbered as per the numbering below,

Please complete the checklist below to verify your submission of the relevant documents:

Schedules	Description	Submitted – Indicate YES or NO
Schedule 1	Proof of registration with National Treasury Central Supplier Database (CSD)	
Schedule 2	Completed and signed SBD Forms	
Schedule 3	Original cancelled cheque or stamped letter from the bank confirming banking details	
Schedule 4	• B-BBEE Verification Certificate/ Sworn Affidavit (full financial year-end of the company should be stated) (Original / Certified Copy) • Proof of documentation required in terms of this RFP to claim points for specific goals	
Schedule 5	TAX Compliance status Pin	

BID SUBMISSION

Bidders are required to submit **one original hard copy and one (1) unlocked USB or CD** with all returnable and electronic copies of bidder's documents as included in the bound printed pack.

AND

Bidders are required to submit their proposal of the RFP documents and response by hand delivery to:

CETA Head Office
52 14th Road
Noordwyk
Midrand
1687

TERMS OF REFERENCE

APPOINTMENT OF A SERVICE PROVIDER FOR FULL TURN-KEY MANAGED INFORMATION AND COMMUNICATION SERVICES FOR THE CETA FOR THREE (3) YEARS. (ICT MANAGED SERVICES)

2. INTRODUCTION

The Construction Education and Training Authority (CETA) invites bids from service providers to provide a comprehensive portfolio of information and communication technology (ICT) services to the CETA. The service provider will be responsible, end-to-end, for the efficient, effective, secure, and modern ICT Environment of the CETA for 36 months. The service provider must assist and guide CETA in improving its ICT environment to serve internal and external stakeholders better.

3. BACKGROUND

The CETA is a Sector Education and Training Authority established in terms of the Skills Development Act, 1998, as amended. The National Skills Development Plan 2030 (NSDP) has five principles and goals that guide the CETA's strategic and annual performance plans.

The CETA recognises the need for a turn-key managed ICT service provider to enhance and unlock the full potential of CETA operations. Currently, the CETA operates manually and is decentralised, leading to inefficient ICT utilisation, relegating ICT to an afterthought rather than a strategic business enabler.

The CETA is looking to elevate the role and use of ICT throughout the organisation, leading with a cloud-first strategy for its digitalisation needs.

The CETA has offices in all 9 provinces and has an organisational structure comprising 180 positions.

4. CETA ORGANISATIONAL STRUCTURE

The CETA organisational structure is currently made up of the following divisions:

3.1 Office of the CEO:

- Risk Management
- Legal and Compliance
- Transformation
- Monitoring and Evaluation
- Special Projects

3.2 Finance

- Supply Chain Management
- Financial Management
- Facilities Management

- The work of this division is supported by SAGE 200

3.3 ETQA and Projects

- Qualifications and Accreditation
- Learning Programmes Implementation and Monitoring
- Client Services and Projects

- The Learner Management System supports the work of this division

3.4 Strategic Support

- Human Resources
- ICT
- Marketing, Communications and Stakeholder Management
- Research, Planning and Reporting

- The Learner Management System and SAGE 300 supports the work of this division

5. OBJECTIVES OF THE CETA- FULL TURNKEY MANAGED ICT SERVICE PROVIDER

Engaging a single managed service provider (MSP) to assist the Construction Education and Training Authority (CETA) with a range of IT services offers several advantages:

1. Streamlined Project Management
    a. Single Point of Contact: Simplifies communication and coordination by providing a single point of contact for all IT-related services, reducing the complexity of managing multiple vendors.
    b. Consistent Communication: Ensures that information is shared consistently and accurately across all services, preventing misunderstandings and misalignments.

2. Cost Efficiency
    a. Bundled Services: Potential for cost savings through bundled services and negotiated discounts for a comprehensive package, as opposed to individual services from multiple vendors.
    b. Reduced Overhead: Lower administrative overhead due to simplified vendor management, invoicing, and contract negotiation processes.

3. Integrated Solutions
    a. Seamless Integration: Ensures all systems and services are integrated and compatible, leading to a more cohesive and efficient IT infrastructure.
    b. Holistic Approach: An MSP with a broad scope can design solutions that consider the interdependencies between different components (e.g., network configuration, endpoint security, and server management).

4. Enhanced Security
    a. Unified Security Strategy: A single MSP can develop and implement a comprehensive security strategy that covers all aspects of the IT environment, eliminating coverage gaps.
    b. Centralised Monitoring: Centralised monitoring and management of security systems (e.g., endpoint security, Mimecast) for quicker detection and response to threats.

5. Expertise and Support
    a. Specialised Knowledge: Access to a team of experts with specialised knowledge across various IT domains, ensuring high-quality installation, configuration, and maintenance.
    b. Proactive Support: Consistent and proactive support and maintenance services that pre-emptively address issues before they become critical.

6. Scalability and Flexibility
    a. Adaptability: Easier to scale services up or down as the organisation's needs change, without the need to negotiate with multiple vendors.
    b. Flexibility: Ability to deploy new technologies and services, as the MSP has a comprehensive understanding of the existing infrastructure.

7. Simplified Compliance and Policy Development
    a. Consistent Policies: Consistent development and implementation of ICT policies across all systems, ensuring compliance with regulatory requirements and organisational standards.
    b. Comprehensive Documentation: Centralised documentation of all processes and policies, aiding in audits and compliance checks.

8. Improved Efficiency and Performance
    a. Optimised Performance: Holistic optimisation of the IT infrastructure, ensuring all components work together efficiently and effectively.
    b. Minimised Downtime: Reduced risk of downtime through coordinated maintenance and support, enhancing overall productivity.

9. Strategic Planning and Futureproofing
    a. Long-Term Planning: Ability to create long-term strategic plans for IT infrastructure development and upgrades, aligning with organisational goals.
    b. Futureproofing: Implementation of scalable and flexible solutions that can adapt to future technological advancements and organisational growth.

10. Comprehensive Reporting and Analytics
    a. Unified Reporting: Consolidated reporting on IT performance, security, and usage, providing clear insights and aiding in decision-making.
    b. Data-Driven Decisions: Use of analytics to inform strategic decisions and improve overall IT governance.

Conclusion:

By engaging a single managed service provider for the installation, configuration, and maintenance of the network, access points, laptops, cell phones, Microsoft 365 E5 suite, endpoint security, Email security, ICT policy development, data room build support, and ongoing support, CETA can benefit from streamlined management, cost efficiencies, integrated solutions, enhanced security, and improved overall performance. This approach enables CETA to focus on its core mission while ensuring a robust and reliable IT infrastructure.

6. PROJECT SCOPE

6.1. Infrastructure Modernisation

6.1.1. Network Architecture Transformation

The service provider must execute a complete transition from our current MPLS-based network to a comprehensive SD-WAN solution:

Current State:

- MPLS connections across nine provincial offices
- Existing business district locations with established connectivity
- Legacy network infrastructure requiring modernisation

Target Architecture:

- Complete SD-WAN deployment with dual-path redundancy
- Cost-optimised connectivity leveraging multiple ISP providers
- Centralised network management with real-time monitoring
- Enhanced security with integrated firewall and threat detection
- Quality of Service (QoS) prioritisation for business-critical applications
- Automatic failover capabilities ensure business continuity

6.1.2. Network Access Control Requirements:

- 802.1X authentication for wired and wireless access
- Device profiling and automatic VLAN assignment
- Guest network isolation with captive portal
- IoT device network segmentation
- MAC authentication bypass (MAB) for non-802.1X devices
- Certificate-based authentication for corporate devices

- Integration with Active Directory/Azure AD
- Rogue device detection and quarantine
- Non-compliant device remediation workflows
- Post-connection health checks (antivirus, OS patches)
- Automated VLAN assignment based on user/device type
- Network visibility for all connected devices
- Contractor/temporary staff access management with expiry
- NAC policy enforcement for BYOD devices
- Quarantine VLAN for non-compliant devices
- Integration with an endpoint security solution
- NAC appliance redundancy and failover

6.1.3. Server and Computing Infrastructure

Head Office Requirements (130 users):

- Modernised server room infrastructure with appropriate cooling and power management
- Virtualised server environment supporting 180+ concurrent users plus intern capacity
- High-availability storage systems with automated backup solutions
- Disaster recovery capabilities within South African data centres

Provincial Office Support (50 users distributed):

- Standardised computing environments across all 9 provinces
- Local backup systems with centralised management
- Remote management capabilities for efficient support

6.1.4. Cloud Strategy and Migration

- Comprehensive cloud adoption framework aligned with cloud-first strategy
- Azure cloud architecture design and implementation
- Cloud migration assessment and roadmap for existing applications
- Multi-cloud strategy and governance (Azure primary, contingency planning)
- Cloud cost optimisation and FinOps implementation
- Cloud security posture management (CSPM)
- Cloud workload protection platform (CWPP)
- Cloud-native application development guidelines
- Infrastructure as Code (IaC) implementation
- Cloud resource tagging and cost allocation strategy
- Cloud backup and disaster recovery strategy
- Hybrid cloud connectivity and integration
- Cloud performance monitoring and optimisation
- Azure landing zones implementation
- Cloud governance policies and compliance monitoring

6.2. Managed ICT Services

6.2.1. Service Desk and Support

- 24/7 technical support with guaranteed response times
- Multi-channel support (phone, email, web portal, mobile app)
- On-site technical support at the Head Office within 4 hours
- Remote support capabilities for provincial offices
- User training and adoption support for new technologies

6.2.2. System Administration and Maintenance

- Complete management of server infrastructure and applications
- Regular security updates and patch management
- Performance monitoring and optimisation
- Capacity planning and scaling recommendations

6.2.3. Capacity Planning and Performance Requirements:

- Quarterly capacity planning reports for all infrastructure
- 12-month capacity forecast for compute, storage, and network
- Performance baseline documentation for all systems
- Trend analysis and growth modelling
- Resource utilisation monitoring and alerting
- Infrastructure right-sizing recommendations
- Capacity planning for user growth (20% year-on-year allowance)
- Network bandwidth utilisation trending and forecasting
- Storage growth analysis and forecasting
- Database sizing and growth projections
- Application performance benchmarking quarterly
- "What-if" scenario modelling for capacity planning
- Capacity constraint identification and remediation plans
- Infrastructure lifecycle management planning (5-year view)
- Monthly capacity management reports to ICT steering committee
- Automated capacity threshold alerting

- Performance optimisation recommendations quarterly

5.2.5 Backup Infrastructure:

- Backup solution supporting all platforms (Windows, macOS, Linux, VMware, Azure)
- Deduplicate and compression ratios documented
- Backup bandwidth management should not impact production
- Backup storage sizing: 30 days retention × 3 copies (3-2-1 rule)
- Off-site backup copy in a geographically separate location

Backup Schedule:

- Tier 1 systems: Hourly incremental, daily full, RPO 1 hour
- Tier 2 systems: 6-hourly incremental, daily full, RPO 4 hours
- Tier 3 systems: Daily incremental, weekly full, RPO 24 hours
- Tier 4 systems: Weekly full backup, RPO 24 hours

Recovery Testing:

- Monthly restore test for random Tier 1 systems
- Quarterly restore test for Tier 2 systems
- Semi-annual restore test for Tier 3/4 systems
- Annual full DR site restore test
- File-level recovery: 95% within 2 hours
- Application-level recovery: 95% within RTO
- Monthly backup report including success rates, capacity, and failed backups

Backup Security:

- Backup data encryption at rest (AES-256)
- Backup data encryption in transit (TLS 1.3)
- Backup administrator access via PAM solution
- Immutable backup copies for ransomware protection
- Air-gapped backup copy updated weekly
- Backup integrity verification daily
- Backup job monitoring and alerting 24/7

6.2.4. Security Management

- Comprehensive cybersecurity, including endpoint protection
- Network security monitoring with 24/7 SOC capabilities
- Regular security assessments and vulnerability management
- Compliance management supporting government regulatory requirements
- Backup and disaster recovery with tested restoration procedures

6.2.5. Software Asset Management and Licensing

- Comprehensive software asset management solution implementation
- Microsoft 365 licence optimisation and management
- Software licence compliance monitoring and reporting
- Licence harvesting and reallocation
- Software usage analytics and optimisation
- Annual software licence true-up and reconciliation

- Software vendor relationship management
- End-of-life software identification and remediation
- Software standardisation and rationalisation
- License cost forecasting and budgeting support
- Software audit preparation and support
- Cloud subscription management (SaaS/PaaS/IaaS)
- Enterprise agreement management
- Software assets register maintenance
- Quarterly licence optimisation recommendations

5.2.5 Print Infrastructure and Management

- Centralised print management solution across all offices (Konica Minolta)
- Secure print release (follow-me printing)
- Print quota management per user/department
- Print cost allocation and chargebacks
- Mobile and cloud printing capability
- Printer fleet monitoring and management (250 users + interns)
- Consumables management and automated ordering
- Print security policies (watermarking, confidential printing)
- Print audit trails for compliance
- Energy-efficient printer settings and monitoring
- Print job reporting and analytics
- Printer driver management and deployment
- Document scanning and digital workflow integration

- Paperless initiatives support
- Monthly print usage reporting by department/user

5.2.6 Business Intelligence and Analytics

- Executive dashboard development (Power BI)
- ICT metrics dashboard (availability, performance, incidents)
- Financial reporting integration from SAGE
- Training and learner analytics from LMS
- Custom report development (up to 30 reports per year)
- Self-service reporting portal for authorised users
- Data warehouse for historical trend analysis
- Predictive analytics for capacity planning
- Mobile BI access (Power BI mobile app)
- Scheduled report distribution
- Report performance optimisation
- User training on BI tools
- Data visualisation best practices implementation
- Integration with Microsoft 365 for collaboration
- Monthly business review reports for executive management

6.3. Business Applications and Systems

6.3.1. Core Business Applications

- Microsoft 365 environment optimisation and management
- Financial management system support
- HR and payroll system integration
- Document management and collaboration platforms

- Skills development tracking and reporting systems

6.3.2. Stakeholder Engagement Platforms

- Public-facing website maintenance and hosting
- Stakeholder portal development and management
- Mobile applications for learner and employer engagement
- Integration with the Department of Higher Education systems

6.3.3. Enhanced Service Desk Capabilities:

- ITIL v4 compliant service desk processes with documented procedures
- Self-service portal with a comprehensive knowledge base (minimum 200 articles)
- AI-powered chatbot for tier-0 support (24/7 availability)
- Mobile service desk app (iOS and Android)
- Remote desktop support tools (TeamViewer, Any Desk or equivalent)
- Automated ticket categorisation and routing
- Service catalogue with 50+ documented services
- Knowledge base search functionality with relevance ranking
- User satisfaction surveys after ticket closure
- Major incident management procedures
- Problem management process with root cause analysis
- Asset management integration with service desk
- Multi-language support (English, Afrikaans, Zulu minimum)
- Video support capability for complex issues
- Screen recording for issue documentation

- Automated escalation based on SLA breaches
- Monthly knowledge base content review and updates
- Service desk dashboard accessible to management (real-time)

6.4. Detailed Technical Infrastructure Specifications

6.4.1. Server Room Environmental Requirements

6.4.1.1. Head Office Server Room Standards:

- **Physical Security:**
  - Biometric access control with audit logging
  - 24/7 CCTV monitoring with 90-day retention
  - Environmental monitoring with real-time alerting
  - Fire suppression system (FM-200 or equivalent clean agent)
  - Water detection sensors with automatic shut-off
- **Power Infrastructure:**
  - Dual-feed power supply from separate utility substations
  - N+1 redundant UPS systems with a minimum 30-minute runtime at full load
  - UPS capacity: Minimum 40kVA for full server room load
  - Generator backup with automatic transfer switch (ATS)
  - Generator fuel capacity: Minimum 72 hours continuous operation
  - Power distribution units (PDUs) with remote monitoring
  - Surge protection and power conditioning
- **Cooling and Climate Control:**
  - Precision air conditioning with N+1 redundancy
  - Target temperature: 18-27°C (ASHRAE standards)
  - Target humidity: 40-60% relative humidity

- Hot aisle/cold aisle containment system
- Temperature and humidity monitoring with alerts
- Backup cooling system for emergencies

- **Structured Cabling:**
  - Category 6A or better for all data connections
  - Fibre optic backbone (single-mode and multi-mode)
  - Cable management system with proper labelling
  - Minimum 30% spare capacity for growth
  - Proper separation of power and data cables

6.4.1.2. Provincial Office Infrastructure:

- Secure lockable network cabinet (minimum 12U)
- Climate control (air conditioning or adequate ventilation)
- UPS protection: Minimum 15-minute runtime
- Environmental monitoring (temperature alerts)
- Basic physical security (lockable cabinet, access control)

6.4.1.3. Advanced Wireless Infrastructure:

- WIFI 6 (802.11ax) access points minimum
- Separate SSID for corporate, guest, and IoT devices
- Guest WIFI with sponsored access and terms acceptance
- Location-based services and WIFI analytics
- Wireless intrusion prevention system (WIPS)
- Rogue AP detection and mitigation
- WIFI capacity planning and heat mapping

- Wireless site surveys for all office locations
- High-density deployment for training rooms (50+ concurrent users)
- WIFI bandwidth management and QoS
- Client device visibility and troubleshooting
- Automatic RF optimisation
- Seamless roaming between APs (fast roaming)
- Guest WIFI bandwidth throttling (10Mbps per user)
- WIFI usage analytics and reporting
- Integration with the NAC solution
- Wireless bridge support for remote areas
- WIFI uptime requirement: 99.5% per office

6.5. Network Security Infrastructure Specifications

6.5.1. Next-Generation Firewall (NGFW) Requirements:

- **Throughput Performance:**
  - Firewall throughput: Minimum 10 Gbps
  - IPS throughput: Minimum 5 Gbps
  - Application control throughput: Minimum 5 Gbps
  - VPN throughput: Minimum 2 Gbps
  - Threat prevention throughput: Minimum 3 Gbps
- **Capacity and Sessions:**
  - Concurrent sessions: Minimum 2 million
  - New sessions per second: Minimum 100,000
  - VPN tunnels: Minimum 500 site-to-site

- SSL VPN concurrent users: Minimum 200
- Maximum throughput with all security features enabled: Minimum 3 Gbps

- **Security Features Required:**
  - Deep packet inspection (DPI) for all traffic
  - Application-level filtering and control
  - Intrusion Prevention System (IPS) with automatic updates
  - Anti-malware and anti-virus scanning
  - SSL/TLS inspection for encrypted traffic
  - Web content filtering with category-based policies
  - Advanced threat protection with sandboxing
  - Geo-blocking and reputation-based filtering
  - DDoS protection and mitigation
  - Zero-day threat protection

- **Management and Visibility:**
  - Centralised management console for all firewalls
  - Real-time traffic visibility and analytics
  - User and application-based reporting
  - High-availability (HA) configuration with automatic failover
  - Virtual firewall support for segmentation
  - API integration for automation

6.5.2. VPN Requirements:

- Site-to-site VPN for all provincial offices
- SSL VPN for remote users (minimum 200 concurrent)
- Multi-factor authentication (MFA) for VPN access
- Split tunnelling capability
- Per-application VPN policies
- Mobile VPN support (iOS and Android)

5.5.3 Identity and Access Management Requirements

- Azure Active Directory Premium implementation and optimisation
- Hybrid identity architecture (Azure AD Connect)
- Single Sign-On (SSO) across all business applications
- Multi-factor authentication (MFA) enforcement for all users
- Conditional access policies based on location, device, and risk
- Privileged Identity Management (PIM) for administrative access
- Just-in-time (JIT) access for elevated privileges
- Identity governance and administration
- Access reviews and attestation (quarterly)
- Privileged access workstation (PAW) implementation
- Password policy enforcement and password less authentication
- Service account management and governance
- Identity protection and risk-based policies
- B2B guest access management
- Self-service password reset (SSPR)
- Identity lifecycle management automation
- Role-based access control (RBAC) framework across all systems

6.6. Security Information and Event Management (SIEM/SOC) Requirements

6.6.1. SIEM Platform Specifications:

- **Log Collection and Retention:**
    - Minimum log sources: 250+ devices and applications
    - Log collection rate: Minimum 5,000 events per second (EPS)
    - Real-time log ingestion with a maximum 5-second delay
    - Hot storage: 90 days of searchable logs
    - Warm storage: 1 year of compressed logs
    - Cold storage: 7 years for compliance (encrypted archive)

- **Log Sources to be Integrated:**
    - All firewalls and network security devices
    - Domain controllers and Active Directory
    - Windows servers and workstations (security events)
    - Linux/Unix servers (syslog)
    - Microsoft 365 (audit logs, email security)
    - Database servers (access and query logs)
    - Application servers and web servers
    - VPN and remote access systems
    - Physical and virtual infrastructure
    - Cloud services (Azure, AWS if applicable)
    - Endpoint protection platforms
    - Network devices (switches, routers, wireless)
- **Correlation and Analytics:**

- Real-time correlation engine with custom rules
- Machine learning and behavioural analytics
- User and Entity Behaviour Analytics (UEBA)
- Advanced threat detection using threat intelligence feeds
- Automated incident creation and prioritisation
- Pre-built correlation rules for common threats
- Custom rule development capability
- Integration with global threat intelligence feeds

- **Incident Response Integration:**
  - Automated playbooks for common security incidents
  - Integration with the ticketing system for incident tracking
  - Case management for security investigations
  - Evidence collection and chain of custody
  - Automated response actions (account lockout, isolation, etc.)
  - Integration with endpoint detection and response (EDR)

6.6.2. Security Operations Centre (SOC) Services:

- **24/7/365 Monitoring:**
  - Dedicated South African-based SOC analysts
  - Three-tier SOC structure (L1, L2, L3 analysts)
  - Minimum 2 analysts per shift
  - Average analyst experience: Minimum 3 years in security operations
- **SOC Service Deliverables:**
  - Real-time security event monitoring and analysis
  - Threat hunting and proactive investigation

- Security incident investigation and response
- Vulnerability correlation with active threats
- Threat intelligence analysis and reporting
- Security metrics and KPI tracking
- Weekly threat briefings
- Monthly executive security reports

- **Response Procedures:**
  - Initial triage: Within 15 minutes of critical alert
  - Incident classification: Within 30 minutes
  - CETA notification: Within 1 hour for high/critical incidents
  - Containment actions: Within 2 hours for critical incidents
  - Full incident report: Within 24 hours of containment

6.7. Endpoint Protection Specifications

6.7.1. Endpoint Detection and Response (EDR) Requirements:

- **Coverage:**
  - All Windows workstations and servers (180+ endpoints + interns)
  - macOS devices
  - Linux servers
  - Mobile devices (iOS and Android)
- **Protection Capabilities:**
  - Next-generation anti-malware with AI/ML detection
  - Behavioural analysis and anomaly detection
  - Exploit prevention and mitigation

- Ransomware protection with automatic rollback
- Zero-day threat protection
- Fileless malware detection
- Script and macro attack prevention
- Memory protection and buffer overflow prevention

- **Detection and Response:**
  - Real-time threat detection and alerting
  - Automated threat containment and isolation
  - Endpoint activity recording (process, network, file)
  - Forensic data collection and analysis
  - Threat hunting capabilities across all endpoints
  - Root cause analysis for security incidents
  - Integration with SIEM for centralised visibility

6.7.2. 5.7.5 Modern Desktop Management

- Windows Autopilot implementation for zero-touch deployment
- Endpoint device lifecycle management (procurement to disposal)
- Automated application deployment (win32, MSIX, LOB apps)
- Windows Update for Business management
- Feature update rings and pilot groups
- Configuration profiles via Intune/GPO
- Desktop-as-a-Service (DaaS) evaluation and implementation if beneficial
- Thin client infrastructure for secure areas (if required)
- Virtual desktop infrastructure (VDI) for remote/intern users (if required)

- Standard operating environment (SOE) design and maintenance
- Application compatibility testing for Windows updates
- Device imaging and deployment automation
- Hardware refresh programme planning and execution
- Device provisioning time target: <30 minutes from box to productive
- Automated driver management and updates

6.7.3. Data Loss Prevention (DLP) Requirements:

- **Data Classification:**
  - Automatic content classification based on sensitivity
  - Support for POPIA data categories (personal information)
  - Custom classification policies for CETA data types
  - Labelling integration with Microsoft 365
- **DLP Controls:**
  - Email DLP (outbound email scanning and blocking)
  - Endpoint DLP (USB, printing, screen capture control)
  - Web/Cloud DLP (upload blocking to unauthorised sites)
  - Network DLP (data in motion monitoring)
  - Policy-based encryption for sensitive data
  - User notification and policy education
- **Device Encryption Requirements:**
  - Full disk encryption (BitLocker or equivalent) for all devices
  - Centralised key management and recovery

- Pre-boot authentication capability
- Removable media encryption enforcement
- Encryption status monitoring and reporting
- Compliance reporting for audit purposes

- **Application Control:**
  - Whitelist/blacklist application management
  - Unsigned application blocking
  - Browser and plugin control
  - Peripheral device control (USB, Bluetooth, etc.)
  - Privilege management and elevation control

6.8. Email Security Requirements

6.8.1. Advanced Threat Protection (ATP) for Email:

- **Anti-Phishing Protection:**
  - URL rewriting and safe links inspection
  - Real-time URL reputation checking
  - Spear-phishing detection using machine learning
  - Business email compromise (BEC) protection
  - CEO fraud and impersonation detection
  - Domain spoofing protection (DMARC, SPF, DKIM enforcement)
- **Malware Protection:**
  - Multi-engine anti-malware scanning
  - Sandbox detonation for suspicious attachments
  - Polymorphic malware detection

- Zero-day attachment protection
- Safe attachments (detonation before delivery)
- Macro and script analysis

- **Content Filtering:**
  - Spam filtering with adaptive learning
  - Adult content filtering
  - Bulk mail detection and filtering
  - Custom keyword and pattern filtering
  - Data loss prevention integration
  - Compliance policy enforcement
- **Email Continuity and Security:**
  - Email quarantine management with user self-service
  - Email encryption for sensitive communications
  - S/MIME and PGP support
  - Email disclaimer management
  - Email archiving with e-discovery (7-year retention)
  - Litigation hold capability
  - Advanced search and retrieval

- **Email Security Monitoring:**
    - Real-time threat dashboard
    - Email security incident alerting
    - User reporting of suspicious emails
    - Security awareness training integration
    - Phishing simulation capabilities
    - Monthly email security reports

6.9. Mobile Device Management (MDM) Requirements

6.9.1. Supported Platforms:

- iOS (iPhone, iPad) - latest 3 major versions
- Android - latest 3 major versions

6.9.2. MDM Core Capabilities:

- **Device Enrolment and Management:**
    - Over-the-air (OTA) device enrolment
    - Bulk enrolment for corporate devices
    - BYOD enrolment with privacy separation
    - Corporate-owned, personally enabled (COPE) support
    - Device inventory and asset tracking
    - Remote device wipe (full and selective)
    - Lost mode and device location tracking

- **Security and Compliance:**
    - Password/PIN enforcement policies
    - Device encryption enforcement
    - Jailbreak/root detection with remediation
    - Compliance policy enforcement
    - Certificate-based authentication
    - Conditional access based on device compliance
    - Mobile threat detection integration
    - Application-level VPN
- **Application Management:**
    - Corporate app store/catalogue
    - Mandatory app deployment
    - App blacklisting and whitelisting
    - App configuration and updates
    - App-level data protection
    - Containerization for corporate data
    - Mobile application management (MAM)
- **Content Management:**
    - Secure document distribution
    - Corporate email configuration (Exchange ActiveSync)
    - Contact and calendar synchronisation
    - Secure browser for corporate resources
    - Remote content wipe (selective wipe)

- **BYOD Support:**
    - Privacy separation (corporate vs personal data)
    - Corporate container with automatic encryption
    - Work profile management (Android Enterprise)
    - Personal app usage monitoring restrictions
    - User consent and privacy policies
    - Self-service portal for device management
    - Reporting and Analytics:
        - Device compliance reporting
        - Application usage statistics
        - Security incident reports
        - Device inventory reports
        - Policy violation alerts
        - User adoption metrics

5.9.4 Mobile PABX/Unified Communications Solution

- Mobile extension integration allows staff to use mobile devices as office extensions
- Fixed-mobile convergence (FMC) solution
- Single number reaches across fixed and mobile devices
- Mobile application providing PBX features (transfer, conference, voicemail)
- Integration with existing mobile contracts
- Least cost routing between mobile and fixed networks
- Mobile presence integration with Microsoft Teams
- Call handover between fixed and mobile devices
- Mobile voicemail integration
- SMS integration for business communications

- Mobile number provisioning and management
- Cost allocation and reporting per user/department
- BYOD mobile PBX client support

5.9.5 Business Voice Recording Requirements

- Selective voice recording for compliance departments (Finance, Legal, HR)
- Recording retention: 7 years in line with POPIA
- Search and playback functionality with role-based access
- Recording encryption at rest and in transit
- Tamper-proof recordings with an audit trail
- Integration with a telephony/VoIP platform
- Recording storage sizing for 180 users' selective recording
- Call tagging and categorisation
- Recording quality assurance (QA) tools
- Legal hold capability for recordings
- Recording backup and DR procedures
- Recording solution compliance with POPIA and ECT Act
- Secure recording access logs
- Recording playback watermarking
- Annual recording compliance audit support

6.10. Unified Communications Requirements

6.10.1. Telephony/VoIP Infrastructure:

- **System Capacity:**
    - Support for 180 permanent users + 70 interns
    - Concurrent call capacity: Minimum 100 calls
    - Voicemail capacity: 100MB per user

- Call recording capacity: 1TB with 12-month retention

- **Features Required:**
  - Auto-attendant and call routing
  - Hunt groups and ring groups
  - Voicemail to email integration
  - Call forwarding and transfer
  - Conference calling (minimum 25 participants)
  - Call hold and park
  - Direct inward dialling (DID) numbers
  - Caller ID and call logs
  - Mobile app for desk phone functionality
  - Softphone support for computers
  - Hot desking capability
- **Quality and Reliability:**
  - QoS configuration for voice traffic
  - Echo cancellation and noise reduction
  - HD Voice codec support (G.722)
  - SIP trunk redundancy
  - Automatic failover to backup trunks
  - Call quality monitoring and reporting

- **Integration:**
  - Microsoft Teams integration (if applicable)

- Contact centre integration (if required)
- CRM integration capability
- Active Directory integration
- Mobile device integration

6.10.2. Video Conferencing Infrastructure:

- **Microsoft Teams Implementation:**
  - Teams' Rooms setup for meeting rooms (minimum 3 rooms at Head Office)
  - Room booking system integration
  - Hardware requirements: Camera, microphone, display, room control
  - Teams Phone System integration
  - Direct Routing configuration (if required)
- **Meeting Room Capabilities:**
  - HD video (minimum 1080p)
  - Multi-camera support
  - Content sharing (wired and wireless)
  - Whiteboard integration
  - Recording and transcription
  - Capacity: 10-25 participants per room
- **Desktop Video Conferencing:**
  - Webcam and headset standards
  - Screen sharing and collaboration tools
  - Virtual backgrounds support

- Meeting recording capability
- Calendar integration
- Mobile app support

- **Network Requirements:**
  - Dedicated bandwidth for video traffic
  - QoS policies for video traffic
  - Network capacity for concurrent meetings
  - Low latency (<50ms) for video traffic
  - Bandwidth management and monitoring

6.10.3. Environmental and Sustainability Requirements

- **Green IT Initiatives:**
  - Energy-efficient hardware specifications (80 Plus Gold PSU minimum)
  - Power management policies for workstations and servers
  - Server virtualisation to reduce physical hardware footprint
  - Data centre PUE (Power Usage Effectiveness) target: 1.5 or better
  - Energy monitoring and reporting for ICT infrastructure
  - Paperless initiatives and digital workflow implementation
  - E-waste disposal according to WEEE (Waste Electrical and Electronic Equipment) regulations

- **E-waste Management:**
  - Environmentally responsible disposal of old equipment
  - Asset sanitisation before disposal (NIST 800-88 standards)
  - Certificate of destruction for disposed equipment

- Equipment recycling and refurbishment, where possible
- Quarterly e-waste disposal reports
- Partnership with a certified e-waste disposal vendor

- **Carbon Footprint:**
    - Annual carbon footprint assessment for ICT operations
    - Cloud services carbon footprint reporting
    - Renewable energy usage is possible for the DR site
    - Video conferencing adoption to reduce travel
    - Energy efficiency recommendations are annually

6.10.4. Data Governance Framework

- **Data Management:**
    - Data classification policy and implementation
    - Data retention schedules aligned with legal requirements
    - Master data management (MDM) for key business entities
    - Data quality monitoring and reporting
    - Data lineage documentation for critical data elements
    - Data stewardship roles and responsibilities
    - Data catalogue for business users
    - Metadata management

- **Data Privacy:**
    - Privacy by design in all new systems
    - Data minimisation strategies
    - Automated data subject request handling (Access, correction, deletion)
    - Consent management system for marketing communications
    - Cookie management and consent on websites
    - Third-party data sharing agreements and monitoring
    - Privacy impact assessment (PIA) for new projects
    - Annual privacy audit

- **Data Architecture:**
    - Enterprise data model documentation
    - Data integration architecture and patterns
    - API-first approach for data access
    - Data lake strategy for analytics (if applicable)
    - Reference data management
    - Data archiving strategy for old systems
    - Legacy data migration standards

6.11. Contact Centre Solution Requirements

6.11.1. Contact Centre Overview:

CETA requires a modern cloud-based or hybrid contact centre solution to support stakeholder engagement activities, including:

- Employer levy queries and support
- Training provided assistance
- Learner inquiries and support
- Grant application guidance
- General CETA information requests
- Contact Centre Capacity:
- Agent Seats: 10 concurrent agent licenses
- Scalability: Ability to scale to 20 agents within 48 hours
- Peak Capacity: Support for 50+ concurrent calls during peak periods
- Queue Management: Unlimited queue capacity with priority routing

6.11.2. Omnichannel Capabilities:

- **Voice (Inbound and Outbound):**
    - IVR (Interactive Voice Response) with customisable menus
    - Automatic call distribution (ACD)
    - Skills-based routing
    - Predictive/preview/progressive dialler for outbound
    - Call recording (100% of calls)
    - Call monitoring and whisper coaching
    - Conference and transfer capabilities
- **Email Management:**

- Unified inbox for all email channels
- Email-to-case conversion
- Automated email routing and assignment
- Email templates and canned responses
- SLA tracking for email responses

- **Web Chat:**
  - Live chat widget for the CETA website
  - Proactive chat invitations
  - Chat-to-voice escalation
  - Chat history and transcripts
  - Co-browsing capability
- **SMS/WhatsApp:**
  - Two-way SMS communication
  - WhatsApp Business integration
  - Automated notifications and reminders
  - Bulk SMS capability for campaigns
- **Social Media Integration:**
  - Facebook Messenger integration
  - Twitter/X monitoring and response
  - LinkedIn message management
  - Unified social media inbox

6.11.3. Intelligent Routing and Workflow:

- **Advanced Call Routing:**
  - Skills-based routing (language, expertise, department)

- Priority routing for VIP stakeholders
- Time-based routing (business hours, holidays)
- Overflow routing to backup queues
- Callback functionality (virtual queue)

- **Workflow Automation:**
  - Business rules engine for complex routing
  - Automated case creation and assignment
  - Escalation workflows for unresolved issues
  - Integration with the ticketing system
  - Screen pop with caller information

6.11.4. CRM and Knowledge Base Integration:

- **Customer Relationship Management:**
  - Integration with existing CRM or provision of CRM capability
  - 360-degree customer view (history across all channels)
  - Contact and company management
  - Interaction history and notes
  - Document attachment capability
- **Knowledge Base:**
  - Searchable knowledge articles (minimum 500 articles)
  - Agent knowledge base interface
  - Self-service customer portal
  - Content management system
  - AI-powered article suggestions

6.11.5. Reporting and Analytics:

- **Real-Time Dashboards:**
    - Live agent status and availability
    - Current queue statistics (waiting, abandoned)
    - Service level achievement (real-time)
    - Agent performance metrics
    - Wallboard displays for agent monitoring
- **Historical Reporting:**
    - Call volume and trends analysis
    - Average handle time (AHT)
    - First call resolution (FCR) rate
    - Customer satisfaction (CSAT) scores
    - Agent productivity reports
    - Abandoned call analysis
    - Service level agreement (SLA) compliance
- **Custom Reports:**
    - Ad-hoc report builder
    - Scheduled report delivery (email/portal)
    - Export to Excel, PDF, CSV
    - API access for custom reporting

6.11.6. Quality Management:

- **Call Recording and Monitoring:**
    - 100% call recording with 12-month retention

- Screen recording capability
- Quality monitoring forms (customisable)
- Random and targeted call sampling
- Evaluation scorecards

- **Performance Management:**
  - Agent performance dashboards
  - Coaching and feedback module
  - Performance improvement plans tracking
  - Gamification and leaderboards
  - Incentive and reward tracking

6.11.7. Workforce Management:

- **Scheduling and Forecasting:**
  - Historical data-based forecasting
  - Multi-skill scheduling
  - Shift management and swap functionality
  - Absence and leave management
  - Adherence monitoring

- **Capacity Planning:**
  - Erlang C calculations for staffing
  - What-if scenario analysis
  - Shrinkage factor calculations
  - Peak period planning

6.11.8. Integration Requirements:

- **Telephony Integration:**
    - Integration with the VoIP system
    - SIP trunk connectivity
    - CTI (Computer Telephony Integration)
    - Screen pop functionality
- **Business Systems Integration:**
    - Microsoft 365 integration (Outlook, Teams)
    - Active Directory for user authentication
    - SharePoint for document management
    - Skills development management system
    - Financial system (for levy queries)
- **Third-Party Integrations:**
    - WhatsApp Business API
    - SMS gateway integration
    - Social media platforms
    - Payment gateway (if required)

6.11.9. Security and Compliance:

- **Data Security:**
    - End-to-end encryption for all channels
    - PCI-DSS compliance (if handling payments)
    - POPIA compliance for customer data

- Role-based access control
- Audit trail for all interactions

- **Quality Standards:**
  - ISO 9001 quality management
  - Disaster recovery capability
  - 99.5% system uptime guarantee
  - Data residency in South Africa

6.11.10. Agent Desktop Requirements:

- **Unified Agent Interface:**
  - Single-pane-of-glass for all channels
  - Intuitive, web-based interface
  - No thick client required (browser-based)
  - Mobile agent capability (iOS and Android)
  - Customisable dashboard widgets
- **Productivity Features:**
  - One-click dialling
  - Automatic call disposition
  - Note-taking and tagging
  - Quick transfer and conference
  - Personal productivity metrics

6.11.11. Self-Service Options:

- **IVR Self-Service:**
    - Natural language IVR
    - DTMF (touchtone) navigation
    - Account balance inquiries
    - Status updates on applications
    - FAQ access via voice
- **Web Portal Self-Service:**
    - Knowledge base access
    - Case submission and tracking
    - Document upload capability
    - Account management
    - Chatbot for common queries

6.11.12. Service Level Requirements:

- Availability: 99.5% uptime during business hours (08:00-17:00 SAST)
- Call Answer Rate: 80% of calls answered within 20 seconds
- Abandonment Rate: Maximum 5% call abandonment
- Email Response: 90% within 24 hours
- Chat Response: 90% within 2 minutes
- SMS Response: 95% within 4 hours
- System Response Time: All transactions within 2 seconds

6.11.13. Training and Support:

- **Agent Training:**
  - Initial system training (2 days)
  - Train-the-trainer programme
  - Online training materials and videos
  - User manuals and quick reference guides
- **Ongoing Support:**
  - 24/7 technical support for system issues
  - Business hours support for user queries
  - Quarterly business reviews
  - Software updates and patches included

6.11.14. Deployment and Implementation:

- **Cloud-Based Deployment Preferred:**
    - No on-premises hardware required
    - Rapid deployment (within 30 days)
    - Automatic updates and maintenance
    - Multi-tenant or dedicated environment
- **Hybrid Option (if required):**
    - On-premises call recording
    - Cloud-based routing and management
    - Data residency in South Africa
- **Implementation Services:**
    - Requirements gathering and design
    - System configuration and customisation
    - Data migration (if applicable)
    - User acceptance testing (UAT)
    - Go-live support (on-site for 5 days)

6.11.15. Change Management Framework and Governance

- Formal change advisory board (CAB) process
- Change management policy and procedures document
- Change classification (standard, normal, emergency, major)
- Change windows: Production changes Saturdays 22:00-06:00 Sunday only
- Emergency change procedures with retrospective CAB review
- Change the calendar visible to all stakeholders

- Change approval workflows based on risk/impact
- Pre-implementation testing requirements for all changes
- Back-out plans are mandatory for all changes
- Post-implementation review within 48 hours of change
- Change success rate target: 95% successful changes
- Change freeze periods (financial year-end, major events)
- Stakeholder communication for changes
- Change management tool integration with the service desk
- Monthly change metrics reporting
- Quarterly CAB review of change policy effectiveness

6.11.16. Quarterly CAB Performance Reviews (Mandatory)

The service provider must conduct a quarterly Change Advisory Board (CAB) performance review covering:

- Change success rates by change type and priority
- Emergency change frequency and root cause analysis
- Failed change analysis with lessons learned
- Change backlog trends and resolution patterns
- Stakeholder feedback on change process effectiveness
- Recommendations for change process improvements
- CAB meeting attendance and participation metrics
- Average time from RFC submission to approval/rejection
- Post-implementation review completion rates

The quarterly CAB review report must be submitted to CETA SM: ICT by the 2nd Friday of the month following quarter-end and presented at the Quarterly Business Review meeting.

6.11.17. The service provider must maintain a Change Advisory Board (CAB)

- All approved and rejected change requests with full documentation
- Change decision rationale and risk assessments
- Post-implementation review results for all changes
- Lessons learned from failed or rolled-back changes
- Change templates and standard change procedures
- CAB meeting minutes and decision records
- Change impact analysis methodologies
- Searchable archive of historical changes (minimum 24 months)

The CAB knowledge base must be:

- Accessible to CETA SM: ICT and designated CETA staff
- Updated within 24 hours of CAB decisions
- Maintained throughout the contract period
- Fully transferred to CETA or successor provider at contract end • Backed up daily with 90-day retention.

6.11.18. The service provider should implement automated CAB workflow tools that provide:

- Automated RFC (Request for Change) submission and routing
- Automated change conflict detection (scheduling conflicts)
- Automated risk scoring based on change attributes
- Digital approvals workflow with email notifications
- Real-time CAB dashboard showing:

  - Pending changes awaiting approval
  - Approved changes scheduled for implementation
  - In-progress changes with status updates
  - Recently completed changes with outcomes
  - Change calendar with conflict alerts
- Integration with an ITSM tool for automated ticket creation
- Automated reminders for post-implementation reviews
- Mobile access for CAB members to review and approve changes

The CAB workflow tool should reduce administrative overhead, improve change visibility, and enable faster decision-making while maintaining proper governance controls.

6.12. Intern Programme IT Support Requirements

6.12.1. Intern User Provisioning Requirements

Annual Intake Management:

- **Capacity Planning:**
  - Support for 50-70 new interns annually
  - Flexible provisioning for staggered intake dates
  - Quick provisioning (within 24 hours of notice)
  - Bulk user creation capability
  - Automated onboarding workflows
- **Account Lifecycle Management:**
  - Automated account creation from the HR system
  - Pre-configured user profiles for intern roles
  - Temporary account with defined expiry dates
  - Automatic extension process for contract renewals
  - Automatic deactivation upon contract expiry
  - Grace period for handover (7 days post-contract)

6.12.2. Intern Onboarding IT Procedures

Day 1 Readiness:

- **Account Provisioning:**
    - Active Directory account creation
    - Microsoft 365 mailbox and applications
    - Network access credentials
    - VPN access (if required)
    - Application access based on role
    - SharePoint/Teams access for collaboration
- **Device Provisioning Options:**
    - **Company-Provided Devices:**
        - Laptop/desktop with standard image
        - Pre-installed software suite
        - Security software and encryption
        - Asset tagging and inventory
        - Peripheral devices (mouse, keyboard, headset)
    - **BYOD (Bring Your Own Device) Programme:**
        - Device compatibility assessment
        - MDM enrolment process
        - Security baseline enforcement
        - Corporate container setup
        - Acceptable Use Policy Agreement
        - Support limitations documentation

- **Initial Setup and Orientation:**
    - IT orientation session (2 hours)
    - Self-service portal introduction
    - Password management training
    - Security awareness briefing
    - Acceptable use policy training
    - POPIA and data protection training

6.12.3. Intern Access Levels and Security Policies

6.12.3.1. Access Control Framework:

- **Standard Intern Access:**
    - Email and Microsoft 365 applications
    - Shared departmental drives (read-only default)
    - Collaboration platforms (Teams, SharePoint)
    - Internet access (filtered and monitored)
    - Intranet and internal resources
    - Learning management system
- **Restricted Access:**
    - No access to financial systems (unless specifically required and approved)
    - No access to HR/payroll systems
    - No administrative rights on any systems
    - No access to sensitive/confidential information (unless justified)
    - Segregation from the permanent staff's sensitive data

- **Department-Specific Access:**
    - Role-based access provisioning
    - Manager approval for additional access
    - Access review at 30-day intervals
    - Audit logging of all access requests
    - Privilege escalation only with justification

6.12.3.2. Security Controls for Interns:

- Enhanced monitoring of intern accounts
- USB device restrictions
- Print monitoring and restrictions
- Email external forwarding is blocked
- Cloud storage upload restrictions
- Social media access restrictions
- Data loss prevention (DLP) policies
- Mandatory security training before system access

6.12.4. Intern Offboarding IT Procedures

6.12.5. Pre-Departure Process:

- **7 Days Before Contract End:**
    - Manager notification of upcoming expiry
    - Data handover reminder
    - Personal file cleanup reminder
    - Exit survey scheduling

- **Final Day Procedures:**
    - Account access revocation (midnight of last day)
    - Email forwarding to manager (30 days)
    - Device return and inspection
    - Asset return verification
    - Access card/credentials collection
    - Exit interview regarding IT systems

6.12.6. Post-Departure:

- **Immediate Actions:**
    - Account deactivation (not deletion)
    - Mailbox conversion to shared mailbox (30 days)
    - OneDrive access transfer to the manager
    - Teams' membership removal
    - VPN access revocation
    - Application license recovery
- **Data Retention:**
    - Email archive: 2 years
    - OneDrive data: Transfer to manager or archive
    - Collaboration data: Retained in shared spaces
    - Audit logs: 7 years retention
    - Account deletion: After 90 days (compliance hold check)

6.12.7. Training Facility IT Requirements (Servers to be supplied by CETA)

- **Network Connectivity:**
    - Dedicated VLAN for training network
    - Isolated from the production network
    - Internet access with content filtering
    - Wireless access (dedicated SSID)
    - Minimum 100Mbps bandwidth
- **Software and Applications:**
    - Standard Microsoft Office suite
    - Industry-specific training software
    - Virtual lab environment (if required)
    - E-learning platform access
    - Assessment and testing platform
    - Screen monitoring/control for the instructor

6.12.8. Training Environment Management:

- Snapshot and restore capability for quick resets
- Standardised training images
- Separate training credentials
- No production data in the training environment
- Sandbox environment for safe learning
- Regular updates and maintenance

6.13. Business Continuity and Compliance Requirements

6.13.1. Business Impact Analysis (BIA) Summary

6.13.1.1. Critical Business Functions:

The following CETA business functions have been assessed for criticality and recovery priorities:

Tier 1 - Critical (RTO: 4 hours / RPO: 1 hour):

- **Financial Management Systems:**
    - Impact of downtime: Unable to process levy payments (R500M+ annually)
    - Revenue impact: R1.5M per day
    - Regulatory impact: Non-compliance with PFMA
    - Recovery priority: Highest
- **Email and Communication Systems:**
    - Impact: Unable to communicate with 500+ employers, training providers
    - Business impact: Grant payment delays, stakeholder dissatisfaction
    - Recovery priority: Highest
- **Skills Development Management System:**
    - Impact: Unable to process learner registrations and training approvals
    - Stakeholder impact: 50,000+ learners and 1,000+ training providers
    - Regulatory impact: DHET reporting non-compliance
    - Recovery priority: Highest

Tier 2 - Important (RTO: 8 hours / RPO: 4 hours):

- **HR and Payroll Systems:**
    - Impact: Unable to process staff payments (180 employees)
    - Business impact: Staff morale, labour relations issues
    - Workaround: Manual payment processing is possible for one cycle
- **Document Management and Collaboration:**
    - Impact: Reduced productivity, delayed approvals
    - Workaround: Email-based collaboration temporarily

- Recovery priority: High

- **Grant Administration Systems:**
  - Impact: Grant processing delays
  - Stakeholder impact: Employer grant payment delays
  - Workaround: Manual processing for urgent cases

Tier 3 - Standard (RTO: 24 hours / RPO: 24 hours):

- Training management systems
- Reporting and analytics platforms
- Intranet and internal portals
- Non-critical file shares

Tier 4 - Low Priority (RTO: 72 hours / RPO: 24 hours):

- Archival systems
- Historical reporting systems
- Test and development environments

6.13.2. System-Specific Recovery Objectives

System / Service	Classification	RTO	RPO	Recovery Strategy
Financial System (ERP)	Critical	4 hours	1 hour	Hot standby, real-time replication
Email (Microsoft 365)	Critical	4 hours	1 hour	Cloud-based HA, multiple data centres
Active Directory	Critical	2 hours	1 hour	Multiple Domain Controller, DR Replication
Skills Development System	Critical	4 hours	1 hour	Database replication, warm standby
HR/Payroll System	Important	8 hours	4 hours	Daily backup, DR site restoration
File Servers	Important	8 hours	4 hours	Daily backup, DR site restoration
SharePoint/Teams	Important	8 hours	4 hours	Microsoft 365 built-in redundancy
Network Infrastructure	Critical	4 hours	N/A	Redundant paths, spare equipment
Internet Connectivity	Critical	2 hours	N/A	Dual ISP, SD-WAN automatic failover
Telephony/VoIP	Important	8 hours	N/A	SIP trunk redundancy, mobile fallback
Training Systems	Standard	24 hours	24 hours	Weekly backup, restore to DR site

6.13.3. Protection of Personal Information Act (POPIA) Compliance

6.13.3.1. POPIA Compliance Framework:

6.13.3.1.1. Lawful Processing Requirements:

- **Consent Management:**
  - Digital consent capture and storage for all data subjects
  - Consent withdrawal mechanism
  - Consent audit trail (who, when, what purpose)
  - Age verification for minor learners
- **Purpose Specification:**
  - Data collection purpose documentation
  - Processing limitation to specified purposes
  - Purpose: change notification process
  - Annual purpose review and update

6.13.3.1.2. Data Subject Rights Management:

- **Right to Access:**
  - Self-service portal for data access requests
  - 30-day response timeframe
  - Identity verification before disclosure
  - Audit trail of access requests
- **Right to Correction:**
  - Online data correction request form
  - Verification and approval workflow
  - 30-day correction timeframe
  - Notification to third parties if shared

- **Right to Deletion:**
    - Deletion request assessment process
    - Legal obligation retention check
    - 30-day deletion timeframe
    - Secure data destruction procedures

6.13.3.1.3. Data Protection Measures:

- **Technical Controls:**
    - **Encryption at rest (AES-256)**
        - Encryption in transit (TLS 1.2+)
        - Access controls based on least privilege
        - Multi-factor authentication for system access
        - Data masking for non-production environments
        - Tokenisation for sensitive identifiers
- **Organisational Controls:**
    - POPIA training for all staff (annual)
    - Data protection impact assessments (DPIAs)
    - Privacy by design in system development
    - Data protection officer (DPO) appointment
    - Third-party data processing agreements
    - Vendor POPIA compliance verification

6.13.3.1.4. Data Breach Management:

- Breach detection and logging mechanisms
- 72-hour breach notification to the Information Regulator
- Data subject notification procedures

- Breach investigation and root cause analysis
- Remediation and prevention measures
- Breach register maintenance

6.13.3.1.5. POPIA Compliance Reporting:

- Quarterly POPIA compliance reports
- Annual data protection audit
- Data processing register maintenance
- Risk assessment and mitigation tracking
- Information officer reporting

6.13.4. Government Minimum Information Security Standards (G-MISS) Compliance

6.13.4.1. G-MISS Framework Implementation:

6.13.4.1.1. Information Classification:

- Top Secret: Not applicable to CETA
- Secret: Not applicable to CETA
- Confidential: Financial data, employee personal information, strategic plans
- Restricted: Internal documents, draft policies, procurement information
- Unrestricted: Public information, published reports

6.13.4.1.2. Access Control Requirements:

- Need-to-know principal enforcement
- Role-based access control (RBAC)
- Segregation of duties
- Access review quarterly
- Privileged access management (PAM)
- Access certification by data owners

6.13.4.1.3. Physical Security:

- Secure areas for sensitive systems (server rooms)
- Access control and visitor management
- CCTV monitoring with retention
- Clear desk and clear screen policies
- Asset disposal procedures
- Secure courier services for media transport

6.13.4.1.4. Incident Management:

- Security incident classification
- Incident response procedures aligned to G-MISS
- Reporting to the relevant government authorities
- Post-incident review and lessons learned
- Incident metrics and trending

6.13.4.1.5. Audit and Compliance:

- Annual G-MISS compliance assessment
- Gap analysis and remediation plans
- Internal security audits (quarterly)
- External penetration testing (annual)
- Security awareness training (mandatory annual)

6.13.5. Development Act IT Requirements

6.13.5.1. Regulatory Reporting Systems:

- **DHET Integration Requirements:**
  - Automated data submission to DHET systems
  - NLRD (National Learner Records Database) integration

- Skills development reporting compliance
- WSP/ATR submission systems support
- Levy payment reporting
- Data Quality and Integrity
- Validation rules for learner data
- ID number verification (Home Affairs integration)
- Qualification verification (SAQA integration)
- Duplicate detection and management
- Data quality metrics and reporting

6.13.5.2. Audit Trail Requirements:

- Complete audit trail for grant administration
- Financial transaction logging
- Learner registration history
- Training provider accreditation tracking
- Appeals and dispute tracking

6.13.5.3. Document Management:

- Learner agreements and contracts (7-year retention)
- Training provider accreditation documents
- Grant application documentation
- Financial records (minimum 7 years)
- Compliance certificates and attestations

6.13.6. Audit and Forensics Requirements

6.13.6.1. Comprehensive Audit Logging:

- Systems Requiring Audit Logs:
- All financial systems (transaction-level logging)
- HR and payroll systems (all changes)
- Email systems (sent/received/deleted)
- File servers (access, modification, deletion)
- Active Directory (all authentication and changes)
- Database systems (all queries and data changes)
- Application systems (user actions and transactions)
- Network devices (configuration changes, access)
- Security systems (all events and alerts)

6.13.6.2. Audit Log Requirements:

- Timestamp (NTP synchronisation)
- User identification
- Source IP address
- Action performed
- Object affected
- Success or failure indication
- Before and after values (for changes)

6.13.6.3. Log Retention and Protection:

- Hot storage: 90 days (online, searchable)
- Warm storage: 1 year (compressed, retrievable)
- Cold storage: 7 years (archived, compliance)
- Tamper-proof log storage

- Log integrity verification (hashing)
- Offsite backup of audit logs
- Encryption of archived logs

6.13.6.4. Forensic Investigation Capabilities:

- **Digital Forensics Tools:**
    - Forensic imaging capability for devices
    - Chain of custody documentation
    - Write-blocking devices for evidence preservation
    - Forensic analysis workstations
    - Memory capture and analysis tools
    - Network packet capture capability
- **Investigation Procedures:**
    - Incident preservation procedures
    - Evidence collection methodology
    - Legal hold implementation
    - Expert witness support capability
    - Court-admissible evidence preparation
    - Investigation reporting templates

6.13.6.5. E-Discovery Requirements:

- Legal hold implementation across all systems
- Advanced search capability across email, files, and databases
- Custodian-based data collection
- PST export and processing

- Early case assessment capability
- Redaction and privilege review support
- Compliance with electronic discovery rules

6.13.6.6. Compliance Audit Support:

- Annual external audit support
- AG (Auditor-General) audit preparation
- Internal audit support (quarterly)
- Regulatory audit support (DHET, Information Regulator)
- System access for auditors (read-only)
- Audit finding remediation tracking

7. SERVICE LEVEL REQUIREMENTS

7.1. Availability and Performance

7.1.1. System Uptime Standards

- Critical systems: 99.5% uptime (maximum 43.8 hours of downtime annually)
- Business applications: 99.0% uptime during business hours
- Network connectivity: 99.5% availability across all locations
- Service desk availability: 24/7/365 with a maximum 15-second response time

7.1.2. Performance Metrics

- Network latency: Maximum 100ms between the Head Office and provincial locations
- Internet bandwidth: Minimum 200Mbps symmetrical at Head Office, 50Mbps at provincial offices
- Service desk resolution:
  - **Priority 1 (Critical): 4 hours maximum**
  - **Priority 2 (High): 8 hours maximum**

- **Priority 3 (Medium): 24 hours maximum**
- **Priority 4 (Low): 72 hours maximum**

7.1.3. Security and Compliance

7.1.3.1. Information Security Requirements

- ISO 27001 certified security management
- Government security clearance, where applicable
- Regular penetration testing and vulnerability assessments
- Incident response procedures with 1-hour notification for critical breaches

7.1.4. Regulatory Compliance

- Protection of Personal Information Act (POPIA) compliance
- Government information security policies adherence
- Skills Development Act reporting requirements support
- National Treasury procurement regulations compliance

8. BIDDER REQUIREMENTS AND QUALIFICATIONS

8.1. Resource Capacity

- Minimum five (5) technical staff with relevant certifications
- 24/7 service desk capabilities/monitoring with a South African presence (Emergency after-hours availability)
- Minimum of two (2) resources on site at CETA Head Office (Midrand) to assist CETA users during office hours
- Senior technical resource available during CETA office hours (Remote)
- The successful bidder must support all CETA Offices country wide.
- The successful bidder must have a local office within Gauteng to support the CETA Head Office based in Midrand, Gauteng, South Africa.

- Dedicated account management and project management resources

9. PROJECT IMPLEMENTATION

9.1. Implementation Phases

Phase 1: Assessment and Design

- Current state assessment and documentation
- Network audit and infrastructure evaluation
- Solution design and architecture documentation
- Migration planning and risk assessment
- Staff readiness evaluation

Phase 2: Infrastructure Deployment

- SD-WAN implementation and testing
- Server infrastructure modernisation
- Security system deployment
- Core system migration and testing
- Staff training programme commencement

Phase 3: Service Integration

- Full managed services activation
- Provincial office integration
- User acceptance testing
- Performance optimisation
- Documentation and knowledge transfer

Phase 4: Stabilisation and Optimisation

- Service level monitoring and adjustment
- User feedback integration

- Performance tuning and optimisation
- Strategic roadmap development
- Contract transition planning

10. PROJECT DURATION

The project is expected to run for a period of three (3) Years, from the award and onboarding of a successful bidder.

CETA requires the outlined services and deliverables for the whole duration of the project.

10.1. Project Handover

- A detailed handover of the developed solution to be made to the CETA towards the end of the contract term, including all project documentation and solution blueprints
- Hand over every phase sign-off to the CETA
- Confirmation that all tasks and responsibilities have been handed over and that the CETA has all necessary information and resources.
- Certificate of CETA ownership of the system, and all data migrated into the system.
- The Solution will be hosted on CETA's platforms.

11. DELIVERABLES

11.1. Project Charter and Project Implementation Plan

11.2. CETA ICT Environment assessment report and recommendations

11.3. Review, Development, and Enhancement of ICT strategies, policies, processes, and guidelines.

11.4. Service Desk, Network and Call Centre Monitoring & Management Tools

11.5. Data migration plan and reporting (where required)

11.6. Training materials (digital) and training workshops to be conducted for internal stakeholders

11.7. ICT Equipment rationalisation and centralization in the newly purpose-built data room.

11.8. Change management plan and progress reports

11.9. Weekly reporting on the performance of the ICT environment (network, backup, security, server room build)

11.10. Ongoing review, recommendation and enhancements of the ICT environment

11.11. Monthly project progress update reports

11.12. End User Support and maintenance (Laptops & systems)

11.13. ICT Environment Security

12. TECHNICAL REQUIREMENTS

Please refer to the "051125 - CETA_Managed_Services_RFP_Requirements.xlsx" document for a complete list of all CETA technical requirements relating to the Managed Services RFP.

BIDDERS WILL BE REQUIRED TO COMPLETE THE ABOVE DOCUMENT AS PART OF THE EVALUATION PROCESS.

13. CETA MANAGED SERVICES APPENDIX LIST

13.1. Appendix 01 – CETA ICT Response Matrix

Priority Level	Response	Resolution	Applicability
Priority 1 (Critical)	15 Mins	1 Hr	24/7/365
Priority 2 (High)	1 Hr	2 Hrs	Business Hours
Priority 3 (Medium)	4 Hrs	8 Hrs	Business Hours
Priority 4 (Low)	8 Hrs	16 Hrs	Business Hours

13.2. Appendix 02 – Service Desk Minimum Service Levels

Service Element	Service Measure	Service Level	Measurement Period
Service Availability	System uptime and availability	99.99%	Monthly
Call answer	Call report	98% of calls are answered within 20 seconds.	Monthly
Email Response	Email response	98% of emails to be logged & assigned within 20 (twenty) minutes of receiving the email	Monthly

Service Element	Service Measure	Service Level	Measurement Period
Abandoned calls	System report	Not to exceed 2% on calls presented to queue. Excluding abandoned calls within the automated Interactive Voice Recognition System.	Monthly
Support Calls and service requests correctly assigned 1st time	Measurement on call assignment before initial response < 3	Correct call assignment for Incident and Service requests. 97%	Monthly

13.3. Appendix 03 – Microsoft Operating Systems

Service Element	Service Measure	Service Level	Measurement Period
Windows server availability	Availability of services	99.90%	Monthly
File services availability	Services availability	99.9%	Monthly
Firmware & software patching for operating system, systems software as well as hardware (drivers, firmware etc.)	Level of firmware and software and supported versions	98% at N-1	Quarterly
Security patching for operating systems, software and hardware (drivers, firmware, etc.)	100% Critical and High Severity	99.90% at N	Monthly
Reporting	Adherence to service reporting requirements including frequency	100% delivery on reporting requirements	Monthly

13.4. Appendix 04 – Local Area & WIFI Network Minimum Service Levels

Service Element	Service Measure	Service Level	Measurement Period
Firmware & software patching and upgrades	100%	N-1	Quarterly
Security patching for firmware and software	100% Critical and High Severity	N	Monthly
Incident Management	Number of Incidents resolved within the resolution times.	97% of all Incidents resolved within the respective resolution times 95% of all Incidents resolved within the respective resolution times	Monthly
Reporting	Adherence to service reporting requirements including frequency	100% delivery on reporting requirements	Monthly

13.5. Appendix 05 – CETA Wide Area Network Minimum Service Levels

Service Element	Service Measure	Service Level	Measurement Period
WAN Backbone Availability	WAN uptime	99.95%	Monthly
HO and branch office availability	Site uptime	99.95 %	Monthly
Latency on the backbone and last mile	Latencies exceeding 150 ms	< 150 ms 100% of the time	Monthly
Packet Delivery on the backbone	Packet loss > 1%	< 1% packet loss, 100% of the time.	Monthly
Jitter on backbone and last mile	Jitter exceeding 30 ms	<30ms, 100% of the time for real-time class of service traffic.	Monthly
Firmware & software patching and upgrades	100%	N-1	Monthly
Security patching for firmware and software	100% Critical and High Severity	N	Monthly
Reporting	Adherence to service reporting requirements including frequency	100% delivery on reporting requirements	Monthly

13.6. Appendix 06 – CETA Offices Nationally and Current Connectivity to be supported

OFFICE	PHYSICAL ADDRESS	Size Of Link
Head Office	52 14th Road	Primary 200 Mb/s
	Noordwyk	Secondary 200 Mb/s
	Midrand	
	1687	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
Gauteng	150 Industrial Road	Primary 50 Mb/s
	Tshwane South TVET College	Secondary 50 Mb/s
	Pretoria West	
	0183	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
Limpopo	73 Biccard Street	Primary 50 Mb/s
	Maneo Building	Secondary 50 Mb/s
	Polokwane Central	
	700	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
Mpumalanga	Disaster Management Building	Primary 50 Mb/s
	COGTA Building	Secondary 50 Mb/s
	R40 Road	
	Nelspruit	
	1200	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
Eastern Cape	No 3 Elton Street	Primary 50 Mb/s
	Southernwood	Secondary 50 Mb/s
	East London	
	5200	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
Free State	Motheo Hillside View TVET	Primary 50 Mb/s
	College Campus	Secondary 50 Mb/s
	Lobona Motsoeneng Street	
	Mangaung	
	Bloemfontein	
	9301	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
KwaZulu-Natal	73 Ramsay Avenue	Primary 50 Mb/s
	Musgrave	Secondary 50 Mb/s
	Durban	
	4001	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
North West	Taletso TVET College	Primary 50 Mb/s
(Mahikeng)	Dr. Albert Luthuli Drive	Secondary 50 Mb/s
	Next to the SABC	
	Mmabatho	
	2790	

OFFICE	PHYSICAL ADDRESS	Size Of Link
North West	Vuselela TVET College Cooperate Centre	Primary 50 Mb/s
(Klerksdorp)	8 Bram Fischer Street	Secondary 50 Mb/s
	Klerksdorp Central,	
	2571	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
Western Cape	Parc du Cap 3	Primary 50 Mb/s
	9-10 Willie Van Schoor Avenue	Secondary 50 Mb/s
	Bellville	
	Cape Town	
	77418	
OFFICE	**PHYSICAL ADDRESS**	**Size Of Link**
Northern Cape	45 Schmidtsdrift Road	Primary 50 Mb/s
	Carters Glen	Secondary 50 Mb/s
	Kimberley	
	8300	

13.7. Appendix 07 – Internet Connectivity Minimum Service Levels

Service Element	Service Measure	Service Level	Measurement Period
Internet Availability	Uptime	99.99% availability	Monthly
Internet Latency	Latency	< 160ms	Monthly
Packet Delivery	% Packet Delivery	100%	Monthly
Reporting	Adherence to service reporting requirements including frequency	100% delivery on reporting requirements	Monthly

13.8. Appendix 08 – Infrastructure Monitoring Minimum Service Levels

This appendix defines the minimum service levels for infrastructure monitoring services as specified in Section 7 of the CETA Managed Services Requirements. The service provider must meet or exceed these service levels throughout the contract period.

Service Element	Service Measure	Service Level	Measurement Period
Monitoring System Availability	Uptime of monitoring platform and tools	99.95% availability of monitoring system 24/7/365	Monthly
Monitoring Coverage - Servers	Percentage of in-scope servers monitored	100% of registered servers with active monitoring agents	Daily
Monitoring Coverage - Network Devices	Percentage of network infrastructure monitored	100% of LAN, Wi-Fi, WAN, and security devices actively monitored	Daily
Monitoring Coverage - Endpoints	Percentage of endpoints with monitoring agents	95% of registered endpoints with active monitoring agents	Weekly
Agent Deployment Time	Time to deploy monitoring agent to new device	Monitoring agent deployed within 2 hours of device registration	Per Device
Critical Alert Response	Response time for critical monitoring alerts	Initial response within 15 minutes, investigation initiated within 30 minutes	24/7/365
High Alert Response	Response time for high priority alerts	Initial response within 30 minutes, investigation initiated within 1 hour	24/7/365
Medium Alert Response	Response time for medium priority alerts	Initial response within 2 hours, investigation initiated within 4 hours	Business Hours
Low Alert Response	Response time for low priority alerts	Initial response within 4 hours, investigation within next business day	Business Hours
Alert Accuracy	Percentage of alerts that are valid (not false positives)	Minimum 85% alert accuracy, quarterly threshold optimization to improve	Monthly
Threshold Configuration Review	Frequency of monitoring threshold optimization	Quarterly review and optimization of all monitoring thresholds with recommendations	Quarterly

Service Element	Service Measure	Service Level	Measurement Period
Anomaly Detection	Detection of abnormal system behaviour	Real-time anomaly detection with automated alerting within 5 minutes of detection	Continuous
Change Detection	Detection of unauthorized or unplanned changes	Real-time change detection with alerting within 5 minutes for infrastructure changes	Continuous
Performance Monitoring - Servers	Server CPU, memory, disk, network monitoring	Real-time monitoring with 1-minute data granularity, alerts at 80% threshold	Continuous
Performance Monitoring - Network	Network bandwidth, latency, packet loss monitoring	Real-time monitoring with 1-minute data granularity, alerts at 75% utilization	Continuous
Network Device Health	Monitoring of device status and health metrics	Real-time health monitoring including temperature, power, fan status with immediate alerts	Continuous
Uptime Monitoring	Device and service availability tracking	Continuous uptime monitoring with 1-minute ping intervals, 99% accuracy	Continuous
ITSM Integration Availability	Uptime of monitoring to ITSM tool integration	99.9% availability of automated incident creation and notification integration	Monthly
Automated Incident Creation	Automatic ticket creation from monitoring alerts	95% of critical and high alerts auto-create ITSM incidents within 2 minutes	Monthly
Monitoring Data Retention	Historical monitoring data availability	12 months online retention for detailed metrics, 24 months for summary data	Continuous
Monitoring Dashboard Availability	Real-time dashboard and reporting portal access	99.9% availability of web-based monitoring dashboards with CETA SM:ICT read-only access	Monthly
System Topology Mapping	Accuracy and currency of infrastructure topology	Automated topology discovery daily, 95% accuracy of documented infrastructure relationships	Daily

Service Element	Service Measure	Service Level	Measurement Period
Capacity Trending Analysis	Trend analysis for capacity planning	Weekly capacity trend analysis with monthly forecasting reports	Weekly/Monthly
Performance Trending Analysis	Performance trend identification and reporting	Daily performance trending with weekly analysis reports identifying optimization opportunities	Daily/Weekly
Monthly Monitoring Report	Comprehensive monthly monitoring report delivery	Detailed infrastructure monitoring report covering availability, performance, health, and capacity delivered by 2nd Friday of following month	Monthly
Quarterly Monitoring Report	Quarterly summary and trend analysis report	Comprehensive quarterly report with rolling 3-month trend analysis delivered by 2nd Friday of following month	Quarterly
Alert Escalation	Timely escalation of unacknowledged alerts	Automatic escalation of critical alerts after 15 minutes, high alerts after 30 minutes	24/7/365
Monitoring Tool Support	Support and maintenance of monitoring platform	24/7 monitoring tool support with 4-hour response for platform issues	24/7/365
Notification Delivery	Successful delivery of monitoring alerts	99.5% successful delivery of email, SMS, and ITSM notifications within 1 minute of alert generation	Monthly
Multi-Site Monitoring	Monitoring coverage across all CETA locations	Centralized monitoring of all 9 provincial offices with 100% coverage	Continuous

Notes:

1. All times specified are in South African Standard Time (SAST) unless otherwise stated.
2. Business Hours are defined as Monday to Friday, 08:00 to 17:00, excluding South African public holidays.
3. 24/7/365 indicates round-the-clock monitoring and response every day of the year, including weekends and public holidays.
4. Continuous monitoring provides real-time monitoring with immediate alert generation upon threshold breaches or anomalies.

5. The monitoring system must provide read-only dashboard access to CETA SM: ICT for real-time visibility of infrastructure health and performance.
6. All monitoring thresholds must be configured in consultation with CETA SM: ICT and optimised quarterly based on trend analysis and operational experience.
7. Monthly and quarterly reports must be delivered by the 2nd Friday of the following month and must include trending analysis for a rolling three-month period.

13.9. Appendix 09 – Cybersecurity Minimum Service Levels

This appendix defines the minimum service levels for all cybersecurity services provided under this managed services contract. The Service Provider must meet or exceed these service levels throughout the contract period.

1. Security Operations Centre (SOC) Availability

Service Element	Service Level	Measurement Period
SOC Operational Availability	99.9% uptime (24/7/365)	Monthly
SOC Staffing Availability	Manned 24/7/365 with qualified analysts	Continuous
SIEM System Availability	99.9% uptime	Monthly
Log Collection Coverage	100% of agreed sources	Monthly

2. Security Incident Response Times

Severity Level	Initial Response	Containment	Resolution Target
Critical (P1)	15 minutes	1 hour	4 hours
High (P2)	30 minutes	2 hours	8 hours
Medium (P3)	2 hours	8 hours	24 hours
Low (P4)	4 hours	24 hours	72 hours

Severity Definitions:

- Critical (P1): Active breach, ransomware, complete system compromise, data exfiltration in progress
- High (P2): Malware infection, attempted breach, privilege escalation, DDoS attack
- Medium (P3): Policy violations, suspicious activity, potential vulnerabilities being exploited
- Low (P4): Minor policy violations, informational alerts, low-risk anomalies

3. Vulnerability Management

Service Element	Service Level	Frequency
Network Vulnerability Scans	100% of network infrastructure	Monthly
Server Vulnerability Scans	100% of servers	Monthly
Endpoint Vulnerability Scans	95% coverage of endpoints	Monthly
Critical Vulnerability Remediation	95% remediated within 7 days	Per scan
High Vulnerability Remediation	90% remediated within 30 days	Per scan
Vulnerability Reporting	Detailed technical + executive reports	Monthly

4. Penetration Testing & Security Assessments

Assessment Type	Frequency
Internal Network Penetration Test	Annually
External Network Penetration Test	Annually
Web Application Security Testing	Annually
Mobile Application Security Testing	Annually (Android & iOS)
Wireless Network Security Testing	Annually
Active Directory Security Assessment	Quarterly

Assessment Type	Frequency
Simulated Phishing Campaigns	Quarterly
Physical Security Assessment	Annually
Post-Assessment Reporting	Within 10 business days

5. Security Awareness Training

Service Element	Service Level	Measurement
Online Training Modules	Monthly modules delivered	100% availability
In-Person Workshops	4 workshops per year	Minimum 80% staff attendance
Training Completion Rate	90% of staff complete monthly modules	Monthly
Training Assessment Pass Rate	85% pass rate on assessments	Per module
Phishing Simulation Click Rate	Reduce to below 5% within 6 months	Quarterly
Training Reporting	Detailed participation & assessment reports	Monthly

6. Threat Intelligence & Monitoring

Service Element	Service Level
Threat Feed Integration	Multiple commercial & open-source feeds
Dark Web Monitoring	24/7 monitoring for CETA-related threats
DNS Monitoring	24/7 monitoring for domain abuse
Social Media Monitoring	24/7 monitoring for brand impersonation
Threat Intelligence Reporting	Weekly summary + immediate critical alerts
Proactive Threat Hunting	Weekly automated + monthly manual exercises

7. Compliance & Reporting

Report Type	Frequency / Timing
Executive Security Dashboard	Real-time access via web portal
Monthly Security Operations Report	By 2nd Friday of following month
Quarterly Security Posture Report	By 2nd Friday of following month
Incident Response Reports	Within 5 business days of resolution
POPIA Compliance Reporting	Quarterly
Audit Support	As needed within 5 business days' notice

8. Anti-Malware & Endpoint Protection

Service Element	Service Level	Measurement
Endpoint Coverage	99% of endpoints protected	Daily
Signature Update Frequency	Updates pushed within 1 hour of release	Continuous
XDR Detection Coverage	Endpoint + Network + Email + Cloud	Continuous
Malware Detection Rate	99.5% detection of known threats	Monthly
False Positive Rate	Below 0.1% of scanned items	Monthly
Quarantine Response Time	Immediate automated isolation	Per detection

9. Service Level Notes

1. Measurement Periods:

- Monthly measurements are based on calendar months.
- Quarterly measurements are based on calendar quarters (Q1: Jan-Mar, Q2: Apr-Jun, etc.)
- Annual measurements are based on the contract year

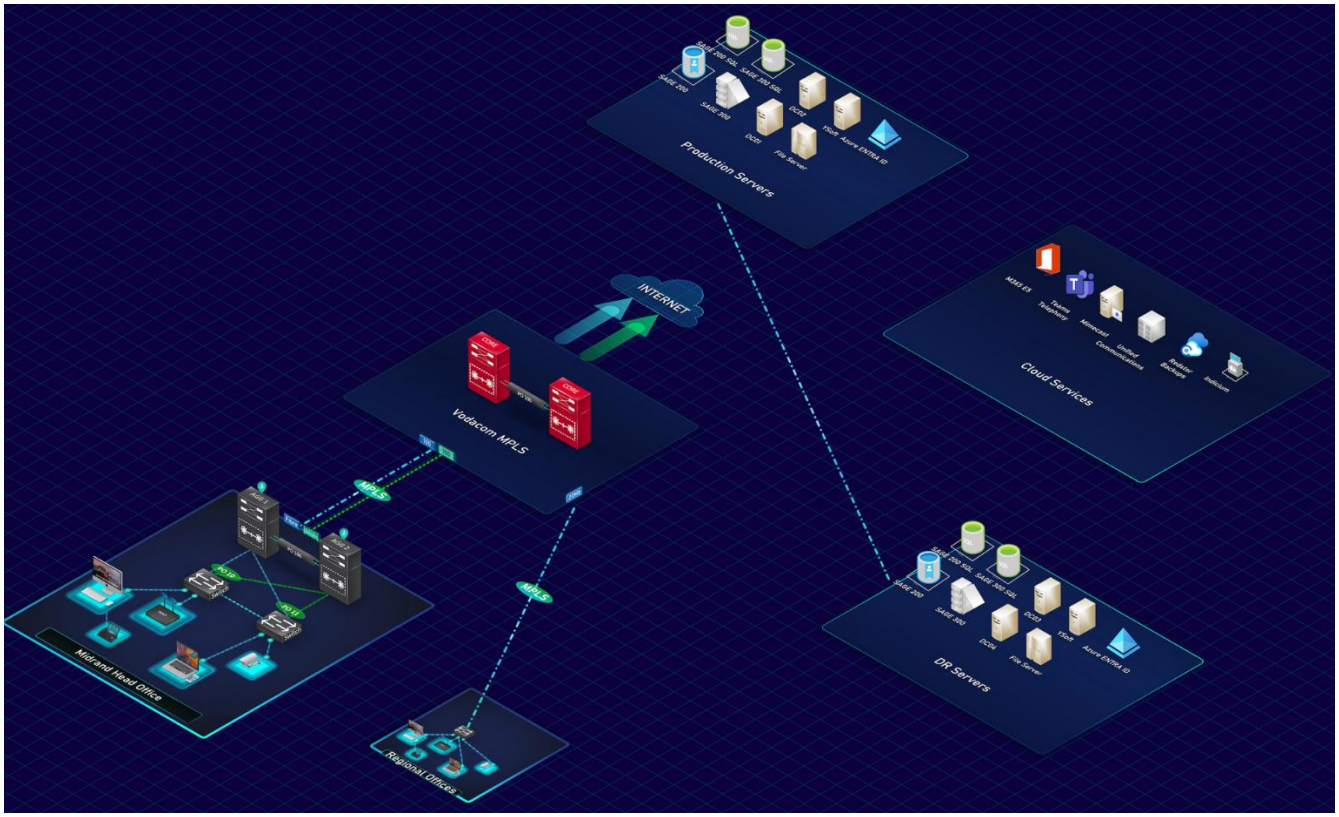
2. SLA Credits:

- Failure to meet critical service levels (SOC availability, P1 response times) results in 5% monthly fee credit per incident
- Persistent failures (3+ months) may result in contract termination provisions

3. Exclusions:

- Planned maintenance windows (with five business days' notice) are excluded from availability calculations.
- Force majeure events as defined in the contract
- Customer-caused incidents or delays in granting access/approvals

CETA Network Diagram



13.10. Appendix 10 – Microsoft Identity (Active Directory) and Azure Active Directory Service Levels

This appendix defines the minimum service levels for Active Directory and Azure Active Directory services as specified in Section 11 of the CETA Managed Services Requirements. The service provider must meet or exceed these service levels throughout the contract period.

Service Element	Service Measure	Service Level	Measurement Period
Active Directory Availability	Uptime of AD domain services	99.99% availability of Active Directory domain services	Monthly
Azure AD (AAD) Availability	Uptime of Azure AD services	99.9% availability of Azure AD services (subject to Microsoft SLA)	Monthly
AD Connect Synchronization	AD to AAD synchronization frequency and success rate	Synchronization every 30 minutes with 99.5% success rate	Daily
User Account Provisioning	Time to create new user accounts	New user accounts provisioned in AD and AAD within 2 hours of approved request	Business Hours
User Account Deprovisioning	Time to disable/delete user accounts	User accounts disabled within 1 hour of request, deleted within 24 hours per retention policy	Business Hours
Password Reset - Standard	Manual password reset response time	Password resets completed within 30 minutes during business hours	Business Hours
Password Reset - Self-Service	SSPR system availability and success rate	99.5% SSPR system availability, 95% successful user self-service password resets	24/7/365
Group Policy Deployment	Time to deploy new or updated group policies	Group policies deployed within 4 hours of approval, effective within next replication cycle	Business Hours
Group Management	Time to create, modify or delete security/distribution groups	Group changes completed within 2 hours of approved request	Business Hours
RBAC Configuration	Azure AD role-based access control changes	RBAC role assignments completed within 2 hours of approved request	Business Hours
Conditional Access Policy	AAD conditional access policy deployment	Conditional access policies deployed within 4 hours of approval with testing	Business Hours

Service Element	Service Measure	Service Level	Measurement Period
Multi-Factor Authentication (MFA)	MFA enrolment support and management	MFA enrolment assistance within 1 hour, 99.5% MFA authentication availability	Business Hours / 24/7
SSO Integration	Single sign-on integration for cloud applications	New SSO integrations completed within 5 business days with testing	Per Request
Identity Protection Alerts	Response to Azure AD identity protection alerts	High-risk alerts responded to within 30 minutes, medium-risk within 4 hours	24/7/365
User Access Reviews	Frequency of access rights audits	Quarterly comprehensive user access reviews with remediation recommendations	Quarterly
Privileged Account Management	Monitoring and management of admin accounts	Daily monitoring of privileged accounts, immediate alerts on suspicious activity	Daily / 24/7
Certificate Management	SSL/TLS certificate monitoring and renewal	90-day advance notice for expiring certificates, renewal completed 30 days before expiry	Continuous
DNS Service Availability	Uptime of DNS services	99.99% availability of internal DNS services	Monthly
DHCP Service Availability	Uptime of DHCP services	99.99% availability of DHCP services with automatic failover	Monthly
AD Replication Monitoring	Monitoring of domain controller replication	Real-time replication monitoring, alerts within 15 minutes of replication failure	Continuous
AD Health Check	Frequency of Active Directory health assessments	Daily automated health checks with weekly detailed reports	Daily / Weekly
Group Policy Object (GPO) Backup	Backup frequency of GPO configurations	Daily automated GPO backups with 90-day retention	Daily
AD Forest Recovery Plan	Maintenance of AD disaster recovery procedures	Annual AD forest recovery plan testing and documentation update	Annually

Service Element	Service Measure	Service Level	Measurement Period
Site and Services Management	AD site topology optimization	Quarterly review of AD sites and services with optimization recommendations	Quarterly
Account Lockout Support	Response time for locked account resolution	Account lockout investigated and resolved within 30 minutes	Business Hours
Password Policy Management	Review and update of password policies	Annual password policy review with compliance verification against security standards	Annually
AD Schema Changes	Testing and deployment of schema modifications	Schema changes tested in non-production, deployed within 10 business days of approval	Per Request
Monthly AD Reporting	Comprehensive monthly AD report delivery	Monthly report covering AD health, user/group changes, admin activity, and compliance delivered by 2nd Friday of following month	Monthly
Quarterly AD Reporting	Quarterly summary and trend analysis	Quarterly report with rolling 3-month analysis delivered by 2nd Friday of following month	Quarterly
Orphaned Account Cleanup	Identification and removal of inactive accounts	Quarterly identification of accounts inactive >90 days with cleanup recommendations	Quarterly

Notes:

1. All times specified are in South African Standard Time (SAST) unless otherwise stated.
2. Business Hours are defined as Monday to Friday, 08:00 to 17:00, excluding South African public holidays.
3. All user account changes (provisioning, deprovisioning, modifications) require approved change requests following CETA's change management process.
4. Azure AD (AAD) availability is subject to Microsoft's cloud service SLA and excludes planned maintenance windows communicated in advance.
5. All security-related changes (RBAC, conditional access, MFA policies) must be tested in a non-production environment before deployment to production.

6. Monthly and quarterly reports must be delivered by the 2nd Friday of the following month and must comply with the reporting structure defined in the main RFP document.
7. Privileged account activity is logged and monitored 24/7/365 with alerts generated for any suspicious or unauthorised activity.Appendix 11 – Storage Systems Service Levels

13.11. This appendix defines the minimum service levels for storage systems management as specified in Section 12 of the CETA Managed Services Requirements. The service provider must meet or exceed these service levels throughout the contract period.

Service Element	Service Measure	Service Level	Measurement Period
Storage System Availability	Uptime of storage arrays and systems	99.99% availability of primary storage systems	Monthly
Storage Performance	I/O response time and throughput	Average read/write latency below 5ms, 99th percentile below 20ms	Monthly
Proactive Monitoring	24/7 monitoring of storage infrastructure	Real-time monitoring with automated alerts within 5 minutes of threshold breach	24/7/365
Storage Configuration Backup	Frequency of storage configuration backups	Daily automated backups of all storage configurations with 90-day retention	Daily
Storage Capacity Monitoring	Tracking and alerting on storage utilization	Real-time capacity monitoring with alerts at 75%, 85%, and 90% utilization	Continuous
Capacity Trend Analysis	Forecasting of storage capacity requirements	Weekly capacity trending with quarterly forecasting and growth projections	Weekly / Quarterly
LUN Provisioning	Time to provision new storage LUNs	New LUNs provisioned and zoned within 4 hours of approved request	Business Hours
LUN Modification	Time to resize or reconfigure existing LUNs	LUN modifications completed within 4 hours of approved change request	Business Hours
Storage Zoning Management	Fabric switch zoning configuration	Zoning changes completed within 2 hours of approved request with validation	Business Hours
Storage Replication	Data replication between primary and DR sites	Continuous replication with maximum 15-minute RPO, 99.9% replication success rate	Continuous

Service Element	Service Measure	Service Level	Measurement Period
Replication Lag Monitoring	Monitoring of replication delays	Real-time replication lag monitoring with alerts if lag exceeds 30 minutes	Continuous
Storage Health Checks	Frequency of comprehensive health assessments	Daily automated health checks with weekly detailed analysis reports	Daily / Weekly
Fabric Switch Availability	Uptime of SAN fabric switches	99.99% availability of SAN fabric infrastructure with redundant paths	Monthly
Storage Incident Response - P1	Response time for critical storage incidents	15-minute initial response, 1-hour resolution initiation	24/7/365
Storage Incident Response - P2	Response time for high priority storage incidents	30-minute initial response, 2-hour resolution initiation	24/7/365
Storage Incident Response - P3	Response time for medium priority storage incidents	2-hour initial response, 4-hour resolution initiation	Business Hours
OEM Engagement	Coordination with storage OEM support	OEM support engaged within 30 minutes for P1/P2 issues, within 4 hours for P3/P4	24/7/365
Storage Firmware Updates	Application of storage firmware patches	Quarterly firmware review, critical patches applied within 30 days of OEM release	Quarterly
Fabric Switch Patching	Firmware updates for SAN switches	Quarterly switch firmware review, updates deployed after-hours with change approval	Quarterly
Storage Compression Management	Monitoring and optimization of compression ratios	Weekly compression ratio analysis with quarterly optimization recommendations	Weekly / Quarterly
Deduplication Monitoring	Tracking deduplication effectiveness	Daily deduplication ratio monitoring with monthly efficiency reports	Daily / Monthly
Bandwidth Management	Replication bandwidth utilization management	Real-time bandwidth monitoring with automatic throttling to maintain 80% max utilization	Continuous

Service Element	Service Measure	Service Level	Measurement Period
Snapshot Management	Storage snapshot creation and retention	Automated snapshots per defined schedule, 30-day retention, 99% snapshot success rate	Daily
Storage Performance Tuning	Optimization of storage performance	Quarterly performance analysis with tuning recommendations and implementation	Quarterly
Storage Path Redundancy	Monitoring of multipath connectivity	Real-time path monitoring with immediate alerts on path failures or degradation	Continuous
Monthly Storage Reporting	Comprehensive monthly storage report delivery	Monthly report covering availability, performance, health, capacity, and trending delivered by 2nd Friday of following month	Monthly
Quarterly Storage Reporting	Quarterly summary and trend analysis	Quarterly report with rolling 3-month analysis and capacity forecasting delivered by 2nd Friday of following month	Quarterly
Storage Disaster Recovery Testing	Validation of storage replication and recovery	Semi-annual DR failover testing with documented results and improvement recommendations	Semi-Annually
Storage Array Upgrades	Planning and execution of storage expansions	Upgrades completed within 10 business days of equipment delivery, zero data loss	Per Request
Storage Documentation	Maintenance of storage environment documentation	Configuration documentation updated within 48 hours of any change, quarterly comprehensive review	Per Change / Quarterly

Notes:

1. All times specified are in South African Standard Time (SAST) unless otherwise stated.
2. Business hours are defined as Monday to Friday, 08:00 to 17:00, excluding South African public holidays.
3. All storage changes (LUN provisioning, zoning, firmware updates) require approved change requests following CETA's change management process.

4. Storage replication RPO (Recovery Point Objective) of 15 minutes applies under normal operating conditions. RPO may be exceeded during maintenance windows or network outages.
5. All storage upgrades and expansions must be performed during scheduled maintenance windows to minimise service impact, with rollback procedures documented and tested.
6. Monthly and quarterly reports must be delivered by the 2nd Friday of the following month and must include trending analysis for a rolling three-month period.
7. OEM support contracts must be maintained for all storage equipment with evidence of valid support agreements provided upon request.
8. Semi-annual DR testing must include documented procedures, test results, failover/failback duration, and any issues identified with remediation plans.

14. PRICING SCHEDULE

14.1. SCOPE OF PROVIDER PRICING - EXCLUSIONS

The following costs are borne directly by CETA and are EXCLUDED from provider pricing in this RFP:

- All software licensing (Microsoft 365, endpoint security, email security, SIEM, backup software, monitoring tools, and all other software)
- All hardware and equipment (servers, storage systems, network devices, switches, routers, wireless access points, firewalls, end-user devices, including laptops, desktops, and mobile phones)
- All telecommunications carrier services (Internet circuits, WAN connectivity, voice circuits, and all other carrier services)
- CETA procures carrier services directly

PROVIDER RESPONSIBILITIES:

The successful bidder is responsible for:

1. Installing, configuring, and managing all CETA-procured solutions
2. Managing carrier relationships and performance monitoring (but not procurement/billing)
3. Providing professional services with a detailed pricing schedule
4. Integrating all systems and services into a cohesive managed environment
5. Ongoing support, maintenance, optimisation and continuous improvement

14.2. CETA INTERNAL CAPABILITY:

CETA has a Microsoft-certified System Administrator and ICT Interns who will work alongside provider resources. The provider must complement this internal capability with additional expertise as required. A clear RACI (Responsible, Accountable, Consulted, Informed) matrix must be developed during implementation to define the division of responsibilities.

INTEGRATION WITH CETA INTERNAL CAPABILITY

CETA employs a Microsoft-certified System Administrator who will be responsible for:

1. Microsoft 365 tenant administration
2. Azure Active Directory management
3. SharePoint and Teams administration
4. Internal systems support

PROVIDER REQUIREMENTS:

1. Work collaboratively with the CETA System Administrator and define clear lines of responsibility
2. Provide complementary expertise (network management, security operations, service desk, and specialised technical support)
3. Facilitate knowledge sharing and skills transfer between the provider and CETA teams.
4. Develop and maintain a clear RACI matrix defining responsibilities
5. Establish joint troubleshooting and escalation procedures
6. Conduct regular coordination meetings (minimum weekly technical sync)

BIDDER SUBMISSION REQUIREMENT:

Bidders must describe:

1. How will they integrate with the internal CETA ICT capability
2. Division of responsibilities between the provider and the CETA teams
3. Collaboration model and communication protocols
4. Handover procedures for routine vs complex issues

10.1.2 TELECOMMUNICATIONS CARRIER SERVICES

CETA procures carrier services directly

CETA RESPONSIBILITIES:

- Procurement and contract management of all telecommunication circuits
- Billing relationships and payment of carrier invoices
- Budget management for carrier costs

PROVIDER RESPONSIBILITIES:

- Technical liaison with service provider for circuit provisioning and installation coordination
- Circuit configuration, testing, and integration with CETA network infrastructure
- Performance monitoring and SLA tracking against service provider commitments
- Fault logging, troubleshooting, and escalation management with service provider
- Capacity planning and upgrade recommendations based on usage analysis
- Monthly carrier performance reporting to CETA SM: ICT
- Optimisation of routing and traffic management across circuits

PROVIDER PRICING:

Bidders must price ONLY for carrier relationship management services. Do NOT include circuit costs in your MRC.

The carrier management fee should cover all activities related to managing CETA's relationship with carrier service provider, including liaison, monitoring, troubleshooting, reporting, and optimisation.

14.3. 10.3 MINIMUM STAFFING REQUIREMENTS

ONSITE RESOURCES (Maximum 3 FTE):

The provider must supply a maximum of THREE (3) dedicated onsite resources.

CETA preference:

1. Service Desk Manager/Lead: 1 FTE
2. Service Desk Analyst: 1 FTE
3. Network Engineer: 1 FTE

OR propose an alternative 3-person team composition with justification.

All onsite resources must be:

1. Based at CETA Head Office, Midrand
2. Available during business hours (8:00-17:00, Mon-Fri)
3. On-call for P1/P2 incidents (24×7)
4. Able to travel to provincial offices as required

SHARED/REMOTE RESOURCES:

In addition to the onsite team, the provider must supply:

1. SOC Analysts: 24×7 monitoring (shared across provider client base)
2. NOC Engineers: Network monitoring and support (shared)
3. Technical Architect: Solution design and escalation (part-time)
4. Account Manager: Contract governance (part-time)
5. Security Specialists: As required for incidents/projects

COLLABORATION WITH CETA ICT:

Provider team will work alongside:

- CETA System Administrator
- CETA Business Analyst
- CETA ICT Interns
- CETA SM: ICT
- Other CETA internal stakeholders

Bidders must detail:

- Proposed team structure and composition
- CVs of proposed key personnel (or profiles if not yet recruited)
- Backup and leave coverage arrangements
- Escalation path within the provider organisation

15. MONTHLY RECURRING CHARGES (MRC)

15.1. SERVICES

Complete the following table with your monthly recurring charges for professional services:

SERVICE CATEGORY	MONTHLY FEE (ZAR)	NOTES / DESCRIPTION
14.1.1 ONSITE PROFESSIONAL SERVICES		
Service Desk Manager/Lead (1 FTE, onsite)	R	Full-time, based at CETA Head Office Midrand
Service Desk Analyst (1 FTE, onsite)	R	Full-time, based at CETA Head Office Midrand
Network Engineer (1 FTE, onsite)	R	Full-time, based at CETA Head Office Midrand
Onsite Services Subtotal	**R**	**Total for 3 onsite FTE resources**
14.2.2 REMOTE/SHARED PROFESSIONAL SERVICES		
SOC Monitoring (24×7 security operations)	R	Shared resource, specify allocated hours/month
NOC Engineering (network monitoring & support)	R	Shared resource, specify allocated hours/month
Technical Architecture & Escalation Support	R	Part-time, as needed for complex issues
Remote Services Subtotal	**R**	**Total for shared/remote resources**

SERVICE CATEGORY	MONTHLY FEE (ZAR)	NOTES / DESCRIPTION
14.2.3 MANAGEMENT & GOVERNANCE		
Account Management	R	Part-time account manager for contract governance
Reporting & Compliance	R	Monthly service reports, quarterly business reviews
Management Subtotal	**R**	**Total for management services**
14.2.4 CARRIER MANAGEMENT SERVICES		
Total Carrier Management (10 sites)	R	Performance monitoring, fault management, reporting
Carrier Management Subtotal	**R**	**Total carrier relationship management**
14.2.5 TOOLS & PLATFORMS		
Service Desk / ITSM Platform	R	Provider-owned ticketing and service management
Remote Monitoring & Management (RMM) Tools	R	Provider-owned monitoring and alerting platform
Backup Management Services	R	Management of CETA-procured backup software
Other Tools (specify): _____	R	Any additional provider-owned tools/platforms
Tools & Platforms Subtotal	**R**	**Total for provider tools and platforms**
TOTAL MONTHLY RECURRING CHARGES (MRC)	**R**	**Grand total - all monthly services**

Notes:

- All prices must be in South African Rands (ZAR), VAT exclusive
- MRC is invoiced monthly in arrears on the last business day of each month
- Carrier costs are procured separately by CETA
- Bidders must price ONLY for carrier relationship management services.

15.2. STAFFING DETAILS

Complete the following table detailing the proposed staffing for CETA:

ROLE	FTE / PART-TIME	LOCATION	QUALIFICATIONS / CERTIFICATIONS	MONTHLY COST
Service Desk Manager/Lead	FTE	Onsite (Midrand)		R
Service Desk Analyst	FTE	Onsite (Midrand)		R
Network Engineer	FTE	Onsite (Midrand)		R
SOC Analysts (24×7)	Shared (min 20 hrs/month)	Remote		R
NOC Engineers	Shared (min 20 hrs/month)	Remote		R
Technical Architect	Part-time (min 20 hrs/month)	Remote		R
Account Manager	Part-time (min 20 hrs/month)	Remote/Hybrid		R
Security Specialists	As needed	Remote		Included above / R
TOTAL MONTHLY STAFFING COST				**R**

**** The hours depicted are for uniform evaluation purposes, actual hours allocation are subject to negotiation with the CETA for the successful bidder. ****

Requirements:

- All onsite resources must be available during business hours (08:00-17:00, Monday-Friday)
- Onsite resources must provide on-call support for P1/P2 incidents (24×7 coverage)
- All onsite resources must be willing to travel to provincial offices as required (travel costs separate)
- Attach CVs or profiles of proposed key personnel (or typical profiles if specific persons have not yet been recruited)
- Describe backup and leave coverage arrangements to ensure continuity
- Provide a clear escalation path within the provider organisation

15.3. ONE-TIME IMPLEMENTATION COSTS (Year 1 Only)

Complete the following table with your one-time implementation costs:

PHASE / DELIVERABLE	DESCRIPTION	COST (ZAR)
PHASE 1: ASSESSMENT & PLANNING (Months 1-2)		
Current State Assessment	Comprehensive assessment of existing ICT environment, asset inventory, network topology, pain points analysis	R
Solution Architecture & Design	Detailed design for all managed services, integration architecture, security framework	R
Migration Planning	Detailed migration plan with timelines, dependencies, risks, and rollback procedures	R
Phase 1 Subtotal		**R**
PHASE 2: IMPLEMENTATION (Months 3-6)		
Service Desk Setup & Configuration	ITSM platform setup, process design, knowledge base creation, integration with CETA systems	R
Network Migration (MPLS to SD-WAN)	Migration of all 10 sites from MPLS to SD-WAN solution, testing, and cutover	R
Security Stack Integration	Integration of CETA-procured security tools (EDR, email security, SIEM), SOC setup	R
Monitoring Platform Deployment	Deployment of monitoring tools across infrastructure, threshold configuration, dashboard setup	R
Microsoft 365 Optimisation	Optimisation of M365 environment, Teams telephony setup, security hardening	R
Provincial Sites Setup	Configuration and deployment of services at all 9 provincial offices	R
Phase 2 Subtotal		**R**
PHASE 3: CHANGE MANAGEMENT (Months 3-8)		

PHASE / DELIVERABLE	DESCRIPTION	COST (ZAR)
Documentation Development	Standard operating procedures, runbooks, configuration guides, disaster recovery plans	R
End-User Training	Training for 180 CETA users on new systems, processes, and service desk procedures and Cyber Security	R
Administrator Training	Technical training for CETA System Administrator and SM: ICT on provider systems and processes	R
Knowledge Transfer	Comprehensive knowledge transfer sessions, shadowing, and handover of critical processes	R
Phase 3 Subtotal		**R**
TOTAL ONE-TIME IMPLEMENTATION COST		**R**

Notes:

- All implementation costs are Year 1 only (one-time charges)
- Payment terms for implementation: Invoiced upon completion of each phase milestone
- Any variations or additional phases must be approved in writing by CETA SM: ICT

15.4. ADDITIONAL SERVICES (Ad-Hoc / Project Work)

Provide hourly rates for work outside the routine managed services scope:

RESOURCE TYPE	HOURLY RATE (ZAR)	DESCRIPTION
Service Desk Analyst	R	Ad-hoc additional support hours
Systems Engineer	R	Ad-hoc systems work, project support
Network Engineer	R	Ad-hoc network projects, site expansions
Security Specialist	R	Security assessments, incident investigations
Technical Architect	R	Solution design, architecture reviews
Project Manager	R	Project coordination and delivery management

Notes:

- Ad-hoc services only provided upon written request from CETA SM: ICT
- Minimum billable increment: _____ hours
- Advance approval required for work exceeding R10,000

15.5. ANNUAL PRICE ESCALATION

Specify your approach to annual price escalation:

☐ **Option A - Fixed Percentage:** _____% per annum (compound escalation)

☐ **Option B - CPI-Linked:** CPI (Stats SA) + _____% per annum

☐ **Option C - Hybrid:** CPI or _____% per annum, whichever is **lower** (capped escalation)

☐ **Option D - Custom:** (describe): _____

Escalation Details:

ITEM	DETAIL
Escalation frequency	☐ Annual on contract anniversary ☐ Other: _____
First escalation date	Month _____, Year _____
Escalation applies to	☐ MRC only ☐ All rates ☐ Other: _____
Notice period	_____ days written notice before escalation takes effect
Documentation required	Price escalation calculation and supporting documentation (e.g., Stats SA CPI certificate) to be submitted _____ days before escalation date

Notes:

- One-time implementation costs (Section 10.4) are fixed and not subject to escalation
- Any escalation above the specified formula requires mutual written agreement
- CETA reserves the right to benchmark rates annually against market standards

15.6. VOLUME DISCOUNTS & MULTI-YEAR COMMITMENT

If applicable, provide any volume discounts or multi-year commitment incentives:

COMMITMENT PERIOD	DISCOUNT OFF TOTAL MRC	CONDITIONS / NOTES
1 year (minimum)	_____%	Baseline contract term, no discount
2 years	_____%	Optional extension, discount off Year 2 MRC
3 years (full term)	_____%	Committed full 3-year term, discount off Years 2-3 MRC

Additional volume incentives:

User count increases:

- 181-200 users: _____% discount on incremental users
- 201-250 users: _____% discount on incremental users
- 251+ users: _____% discount on incremental users

Site additions:

- Per additional provincial site: R _____ per site per month
- Discount for multiple site additions (3+ sites): _____%

Notes:

- Discounts are cumulative (multi-year + volume)
- Any scope increases are subject to a formal change request and pricing approval.
- Volume discounts apply to new users/sites only, not base pricing

---

15.7. THREE-YEAR PRICING SUMMARY

Complete the three-year total cost summary:

ITEM	YEAR 1	YEAR 2	YEAR 3	3-YEAR TOTAL
Monthly Recurring Charges (MRC)				
MRC per month (from Section 10.2)	R	R	R	
Number of months	**12**	**12**	**12**	**36**
Annual MRC subtotal	R	R	R	R
One-Time Implementation				
Implementation cost (from Section 10.4)	R	R 0	R 0	R
Price Escalation				
Escalation rate (from Section 10.7)	Base year	+ _____%	+ _____%	
Escalation applied to MRC	Base	Escalated	Escalated	
ANNUAL TOTALS	**R**	**R**	**R**	
THREE-YEAR CONTRACT TOTAL				**R**

Notes:

- All amounts are ZAR, VAT exclusive
- Payment terms: Net 30 days from invoice date
- CETA reserves the right to invoke early termination clauses as per GCC

15.8. PAYMENT TERMS & CONDITIONS

15.8.1. Monthly Recurring Charges:

- Invoiced monthly in arrears on the last business day of each month
- Payment due within 30 (thirty) days of invoice date
- The invoice must detail services rendered, any ad-hoc work, and expenses (if applicable)
- The monthly service report must accompany the invoice

15.8.2. Implementation Milestone Payments:

- Phase 1 (Assessment & Planning): Invoiced upon completion and acceptance, payable within 30 days
- Phase 2 (Implementation): Invoiced per milestone completion and acceptance, payable within 30 days
- Phase 3 (Change Management): Invoiced upon completion and acceptance, payable within 30 days
- Holdback: CETA reserves the right to withhold _____% of implementation costs until final acceptance

15.8.3. Ad-Hoc Services:

- Invoiced monthly based on actual hours worked and pre-approved by CETA SM: ICT
- Timesheets must accompany the invoice with a description of the work performed
- Payment due within 30 days of invoice date

15.8.4. Disputed Invoices:

- CETA will pay undisputed portions within 30 days
- Disputed items will be escalated to the Account Manager for resolution
- Resolution timeframe: _____ days from dispute notification
- Interest on late payments (if applicable): Prime rate + _____% per month on overdue amounts

15.8.5. SLA Credits:

- SLA penalties/credits will be calculated monthly and deducted from the next month's invoice
- Details of SLA breaches and credits must be included in the monthly service report
- Refer to Appendices 01-11 for specific SLA credit calculations

---

15.9. PAYMENT SCHEDULE EXAMPLE (Illustration Only)

This example illustrates how payments would flow over the contract term:

PERIOD	SERVICES DELIVERED	AMOUNT	CUMULATIVE
YEAR 1			
Month 1	Assessment & Planning	R _____ (Impl.)	R _____
Month 2	Assessment + MRC (50%)	R _____ + R _____	R _____
Months 3-4	Implementation + MRC (75%)	R _____ + R _____	R _____
Months 5-12	Full MRC (8 months)	R _____ × 8	R _____
Year 1 Total		**R _____**	**R _____**
YEAR 2			
Months 13-24	Full MRC + Escalation	R _____ × 12	R _____
Year 2 Total		**R _____**	**R _____**
YEAR 3			
Months 25-36	Full MRC + Escalation	R _____ × 12	R _____
Year 3 Total		**R _____**	**R _____**
CONTRACT TOTAL (36 Months)			**R _____**

PERIOD	SERVICES DELIVERED	AMOUNT	CUMULATIVE
VAT			
Contract total VAT Inclusive			

15.10. PRICING NOTES & CONDITIONS

15.10.1. Price Validity:

All prices quoted must remain valid and binding for **180 days** from the RFP submission deadline.

15.10.2. Pricing Transparency:

Bidders must provide complete transparency on all pricing components. No hidden fees or charges are permitted. The provider must absorb any costs not explicitly detailed in this pricing schedule.

15.10.3. Third-Party Costs:

If the provider subcontracts any services (e.g., specialised security services, carrier management), these costs must be itemised separately in your proposal with the subcontractor identified.

15.10.4. Scope Changes:

Any material changes to scope (e.g., significant user count changes, additional sites, new services) will be subject to a formal change control process and pricing adjustments via written amendment.

15.10.5. Cost Savings:

If the provider identifies opportunities for cost savings or operational efficiencies that benefit CETA financially, a gainshare arrangement may be negotiated separately. Provider must document the savings methodology and obtain CETA approval before implementation.

15.10.6. Benchmarking:

CETA reserves the right to conduct annual pricing benchmarking against market rates. If provider pricing is found to be more than _____% above market rates, CETA may request renegotiation or invoke market adjustment clauses.

15.10.7. Currency:

All pricing must be in South African Rands (ZAR). Foreign currency pricing is not permitted.

15.10.8. VAT:

All prices quoted must be **VAT exclusive**. VAT will be added as applicable per South African tax law.

15.11. 10.13 PRICING SUBMISSION CHECKLIST

Before submitting your pricing, please confirm:

- All pricing tables in Sections 10.2 - 10.9 are completed with specific ZAR amounts (no blanks or TBDs)
- The three-year total (Section 10.9) does not exceed R21,000,000 unless clearly justified
- Pricing excludes all items listed in Section 10.1 (Exclusions)
- Staffing details and qualifications provided in Section 10.3
- Annual escalation methodology is clearly specified in Section 10.7
- Payment terms understood and accepted per Section 10.10
- All assumptions, exclusions, and conditions are clearly documented
- Pricing is valid for 180 days from the submission date
- Any third-party or subcontractor costs are itemised and disclosed
- Signed declaration: "I certify that the pricing submitted is accurate, complete, and binding for the period specified."

END OF PRICING SCHEDULE

Note to Bidders: Failure to complete all sections of this pricing schedule accurately and comprehensively may result in disqualification or forfeiture of evaluation points. Ensure all monetary values are clearly stated in South African Rands (ZAR), VAT exclusive.

NB: Mandatory system updates and enhancements are to be considered annually by the appointed service provider, to be specified/developed per the identified need of the CETA, at no additional cost to the CETA.

Please note the hourly rates given above are estimates and are only for comparison and evaluation purposes, they may increase depending on the needs during the project. The submitted prices must be fixed for a period of twelve months.

…….. ……

Signature Date

…… ……

Position Name of Bidder

16. EVALUATION CRITERIA

16.1. Criterion 2 – Functionality:

Functionality is worth 100 points. The minimum threshold is 65 points. Applicants who score less than 65 points on functionality will therefore be disqualified. Those who score 65 points or more will be further evaluated on a demonstration/presentation of their capability.

Functionality Evaluation Criteria:

Reference Letters Applicants must have specific experience and submit contactable references of similar work undertaken.	**Total – 10 points**
Reference Letter Requirements • Reference Letters must be on a client's letterhead with contactable details provided. • Reference letters with redacted, or otherwise illegible detail will result in them being found invalid and will not be considered for reference letter points. • Reference letters may not be more than five (5) years old from the date of publication of this tender. • Bidder reference letters are subject to verification by the CETA.	
Reference Letter Points Allocation:	**Points Awarded**
Scoring: • Submission of five (5) or more reference letters contactable references of similar work undertaken. (**10 Points**) • Submission of two (2) to four (4) reference letters contactable references of similar work undertaken. (**5 Points**) • Submission of one (1) reference letter contactable references of similar work undertaken. (**1 Point**) • No reference letters meeting CETA contactable references of similar work undertaken. (**0 Points**)	

Technical Proposal Bidders are required to submit a detailed technical proposal.	**Total – 50 points**
The Technical Proposal must comprehensively demonstrate the bidder's ability to provide a solution in alignment with the requirements listed in this document.	
Technical Proposal Points Allocation:	**Points Awarded**
Technical Requirements Compliance Description: Demonstrate the proposed solution/s compliance with the technical requirements listed in the "20251105_Managed Services_ RFP_Requirements.xlsx" document. A minimum threshold of 70% compliance with the technical requirements listed in the "051125 - CETA_Managed_Services_RFP_Requirements.xlsx" document is required to score points for this evaluation criteria. **Scoring:** • Proposed solution/s meets **90%** or higher compliance with the technical requirements listed in the "051125 - CETA_Managed_Services_RFP_Requirements.xlsx" document. (**50 points)** • Proposed solution/s meets **80% to 89.99%** compliance with the technical requirements listed in the "051125 - CETA_Managed_Services_RFP_Requirements.xlsx" document. (**40 points)** • Proposed solution/s meets **70% to 79.99%** compliance with the technical requirements listed in the "051125 - CETA_Managed_Services_RFP_Requirements.xlsx" document. (**30 points)** • Proposed solution/s does not meet the minimum required **70%** compliance with the technical requirements listed in the "051125 - CETA_Managed_Services_RFP_Requirements.xlsx" document. (**0 points)**	
Project Team Composition Bidders are required to submit a proposed project team with resources meeting the requirements of the CETA.	**Total – 20 points**

Project Team Requirements: • The proposed Project Team must be comprised of 80% (eighty percent) South Africans (Citizen and or Permanent Resident). • Copies of South African Identity Documents must be provided for all South African (Citizen and or Permanent Resident) project team members. Failure to provide certified copies of project team member South African identity documents will result in them being found invalid, and they will not be considered for project team composition points. • Copies of Passports for Non-South African Project Team members must be provided. • Each Project team members CVs must include a summary page indicating the role they will fulfil on the project. • Each Project team members CVs must include supporting evidence of having performed work in line with the role they are proposed for on the project. • Each project team members must have a minimum of five (5) years' experience in the role they are proposed for on the project. **Project Team Disclaimer:** • Only proposed project team members, and alternates, for which CV's and copies of identity documents or passports are received, will be considered by CETA in the event a bidder is successful. • The successful bidder may not substitute project team members with ones that were not included in their original bid response, unless agreed upon by the CETA. • The successful bidder will be required to provide certified copies of South African IDs or Passports upon award.	
Project Team Roles Required (Hybrid requirement Remote/Onsite): 1. Project Manager 2. IT Service Desk Specialist 3. IT Service Desk Administrator (X2) 4. Infrastructure/Systems Engineer 5. Network Engineer 6. Cloud Services Engineer 7. Cyber Security Specialist 8. Solution Architect 9. Change Manager	

10. Training Manager	
Project Team Points Allocation:	**Points Awarded**
Scoring: • 8 or more Valid CETA Project Team requirements have been met, with suitable CVs for required role experience are provided for the Project Team Roles. (**20 Points**) • 5 - 7 Valid CETA Project Team requirements have been met, with suitable CVs for required role experience are provided for the Project Team Roles. (**10 Points**) • 4 - 3 Valid CETA Project Team requirements have been met, with suitable CVs for required role experience are provided for the Project Team Roles. (**5 Points**) • Less than 2 Valid CETA Project Team requirements have been met, with suitable CVs for required role experience are provided for the Project Team Roles. (**0 Points**)	

16.2. Criterion 3 – Demonstration / Presentation

Bidders who score 65 points or more in functionality will be invited to a Demonstration/Presentation of their proposed solution (s).

The Demonstration /Presentation will be worth 20 points, and bidders need to score at least 15 points to be further evaluated on price and preference. Bidders who score less than 15 points will be disqualified.

Refer to the Rating Scale table in this section for clarification on the Excellent, Good, Acceptable, Reservations and Unacceptable ratings.

Demonstration / Presentation Criterion	Total Points - 20
PART A – Contact Centre (**4 points**) • Demonstration / Presentation on the Contact Centre solution o Excellent – **4 points** o Good – **3 points** o Acceptable – **2 points** o Minor Reservations – **1 Point** o Serious Reservations / Unacceptable – **0 Points**	
PART B – Omnichannel Help Desk (**4 points**) • Demonstration / Presentation on the Omnichannel Help Desk solution o Excellent – **4 points** o Good – **3 points** o Acceptable – **2 points** o Minor Reservations – **1 Point** o Serious Reservations / Unacceptable – **0 Points**	
PART C – Mobile PBX (**4 points**) • Demonstration / Presentation on the Mobile PBX solution o Excellent – **4 points** o Good – **3 points** o Acceptable – **2 points** o Minor Reservations – **1 Point** o Serious Reservations / Unacceptable – **0 Points**	
PART D – Microsoft Teams Origination and Termination (**4 points**) • Demonstration / Presentation on Microsoft Teams Origination and Termination o Excellent – **4 points** o Good – **3 points** o Acceptable – **2 points** o Minor Reservations – **1 Point** o Serious Reservations / Unacceptable – **0 Points**	

PART E – Cyber Security (**4 points**) • Demonstration / Presentation on the Cyber Security solution o Excellent – **4 points** o Good – **3 points** o Acceptable – **2 points** o Minor Reservations – **1 Point** o Serious Reservations / Unacceptable – **0 Points**	

Rating Scale that CETA Bid Evaluation Committee (BEC) Members may choose to utilise:

Rating	Definition	Score
Excellent	**Exceeds** the requirement. Exceptional demonstration by the supplier of the relevant ability, understanding, experience, skills, resource and quality measures required to provide the goods / services. Response identifies factors that will offer potential added value, with supporting evidence.	**4**
Good	**Satisfies** the requirement with **minor additional benefits**. Above average demonstration by the supplier of the relevant ability, understanding, experience, skills, resource and quality measures required to provide the goods / services. Response identifies factors that will offer potential added value, with supporting evidence.	**3**
Acceptable	**Satisfies** the requirement. Demonstration by the supplier of the relevant ability, understanding, experience, skills, resource, and quality measures required to provide the goods / services, with supporting evidence.	**2**
Reservations	Satisfies the requirement with **reservations**. Some minor reservations of the supplier's relevant ability, understanding, experience, skills, resource and quality measures required to provide the goods / services, with little or no supporting evidence.	**1**
Unacceptable	**Does not meet the requirement**. Does not comply and/or insufficient information provided to demonstrate that the supplier has the ability, understanding, experience, skills, resource & quality measures required to provide the goods / services, with little or no supporting evidence.	**0**

16.3. **Criterion 3** – Price and Preference Evaluation

Bidders who score a minimum of 15 points or more on presentations will be further evaluated in terms of Price and Preference points (B-BBEE status level of contributor and specific goals allocated points). As per the table below, price is evaluated over 80 points and preference points over 20:

The specific goals allocated points	Criteria	Number of points allocated. (80/20 system)	Number of points claimed(80/20 system) (To be completed by the bidder)	Form of evidence
B-BBEE contribution level score of the bidder	B-BBEE Level 1	10		CIPC document, valid BBBEE certificate/sworn affidavit.
	B-BBEE Level 2	8		
	B-BBEE Level 3	6		
	B-BBEE Level 4	4		
	B-BBEE Level 5-6	2		
	B-BBEE Level 7-8	1		
	Non-compliant contributor	0		
CETA transformation strategic position to empower designated groups in line with the Transformation Policy	100% - 51% Women Ownership	5		CIPC document, valid BBBEE certificate/sworn affidavit and CSD report
	51% - 35% Women Ownership	3		
	35% - 20% Women Ownership	1		
	100% - 51% Youth Ownership	5		
	51% - 35% Youth Ownership	3		

	35% - 20% Youth Ownership	1		

Whilst CETA is issuing this invitation in good faith, it reserves the right to cancel or delay the selection process at any time without providing reasons therefore and reserves the right not to select any of the respondents to this invitation.

BID NO: 009-2025/2026 terms of reference were approved as follows:

Name……...Signature:…….Date:……
BSC Chairperson

17. ADMINISTRATIVE ENQUIRIES

ANY ENQUIRIES REGARDING THE BIDDING PROCEDURE MAY BE DIRECTED TO:

Department: Supply Chain Management Unit

Contact Person: Dr Sibusiso Sifunda

Tel: 011 265 5901

E-mail: scmtenders@ceta.co.za and CC Sibusisos@ceta.co.za

Kindly note that your technical enquiries will be facilitated by SCM between the service provider and the relevant CETA project lead.

SBD 1 - PART A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE (*NAME OF DEPARTMENT/ PUBLIC ENTITY*)					
BID NUMBER:	BID NO: 009 – 2025/2026	CLOSING DATE:	27 January 2026	CLOSING TIME:	11H00
DESCRIPTION	**APPOINTMENT OF A SERVICE PROVIDER FOR FULL TURN-KEY MANAGED INFORMATION AND COMMUNICATION SERVICES(ICT) FOR THE CETA FOR THREE (3) YEARS**				

BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT *(STREET ADDRESS)*

CETA Head Office
52 on 14th Road
Noordwyk
Midrand

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO		**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**	
CONTACT PERSON		CONTACT PERSON	
TELEPHONE NUMBER		TELEPHONE NUMBER	
FACSIMILE NUMBER		FACSIMILE NUMBER	
E-MAIL ADDRESS		E-MAIL ADDRESS	

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

ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES OFFERED?	☐Yes ☐No [IF YES ENCLOSE PROOF]	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: ……

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**

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

SBD 6.1

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**

(*delete whichever is not applicable for this tender*).

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

b) The 80/20 preference point system will be applicable in this tender. The lowest/ highest acceptable tender will be used to determine the accurate system once tenders are received.

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	80
SPECIFIC GOALS	20

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

2.1 "Acceptable bid or acceptable quotation" means a bid or quotation which in all respects complies with the specifications and Conditions of Tender as set out in the tender document.

2.2 "Black people" means Africans, Coloureds and Indians (refer to the B-BBEE Act for more details)

2.3 "B-BBEE" means broad-based black economic empowerment as defined in section 1 of the Broad-Based Black Economic Empowerment Act;

2.4 "B-BBEE status level of contributor" means the B-BBEE status of an entity in terms of a code of good practice on black economic empowerment, issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act;

2.5 "bid" means a written offer in a prescribed or stipulated form in response to an invitation by an organ of state for the provision of goods or services, through and advertised competitive bidding processes or proposals;

2.6. "Broad-Based Black Economic Empowerment Act" means the Broad-Based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003);

2.7. "Control" means the possession and exercise of legal authority and power to manage the assets, goodwill and daily operations of a business and the active and continuous exercise of appropriate managerial authority and power in determining the policies and directing the operations of the business.

2.8. "Disability" means, in respect of a person, a permanent impairment of a physical, intellectual, or sensory function, which results in restricted, or lack of, ability to perform an activity in the manner, or within the range, considered normal for a human being AND is in procession of a proof of disability.

2.9. "EME" means an Exempted Micro Enterprise in terms of the relevant code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;

2.10. "Locality" means that the enterprise has either its head office or an operational office located in a township or rural area AND they are in procession of a municipal account, not older than three months for that location.

2.11. "military veteran" means has the meaning assigned to it in Section 1 of the Military Veterans Act, 2011 (Act No. 18 of 2011).

2.12. "Ownership" of an enterprise has the meaning defined in the Ownership Element of the B-BBEE Amendment Act of 2013 and the codes of good practice. This includes exercisable

voting rights in the enterprise; economic interest in the enterprise (including Employee Share Ownership Programmes, Broad-based Ownership Schemes).

2.13. **"price"** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;

2.14. "**Proof of B-BBEE status level of contributor**" means:

a) B-BBEE Status level certificate issued by an authorized body or person (such as a SANAS verification agent);

b) A sworn affidavit as prescribed by the B-BBEE Codes of Good Practice;

c) A CIPC B-BBEE certificate; or

d) Any other requirement prescribed in terms of the B-BBEE Act.

2.15. **Proof of Disability**" means:

a) A completed SARS "Confirmation of Diagnosis of Disability" form endorsed by a duly registered medical practitioner which will remain valid for 10 years where the disability is of a permanent nature;

b) A medical report and functional assessment report confirming the disability; or

c) A SASSA disability grant.

2.16. "**Proof of Locality**" means:

a) A municipal rates invoice in the name of the company submitting the quotation that has been issued within the last three months;

b) An affidavit or equivalent from an authorised traditional leaders or local councillor in regions where municipal rates invoices are not available, showing the township name and ERF number or physical address;

c) A signed lease with a property owner located in that municipality/township (CETA may request a recent statement from the landlord);

d) A utilities rates statement (examples, Eskom or Telkom fixed line service) showing the physical address and name of the company or director's name

2.17. "**Proof of Military Veteran**" means a:

a) Military veteran certificate as issued by the Department of Military Veterans in the name of the individual; or

b) Military veteran certificate as issued by the Department of Military Veterans in the name of the company.

2.18. "**Proof of Ownership**" means:

a) The % ownership indicated on the Central Supplier Database. The CSD integrates with the systems at Home Affairs (demographic information); Companies and Intellectual Property Commission (CIPC) (for company information such as shareholding); and other databases (such as the banks).

2.19. **"QSE"** means a qualifying small business enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;

2.20. "**Rand value**" means the total estimated value of a contract in Rand, calculated at the time of the tender invitation.

2.21. "**Specific Goals**" means those goals as contemplated in section 2(1)(d) of the PPPFA which may include contracting with persons, or categories of persons, historically disadvantaged by unfair discrimination on the basis of race, gender and disability

including the implementation of programmes of the Reconstruction and Development Programme as published in Government Gazette No. 16085 dated 23 November 1994

2.22. **"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

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

2.24. **"township"** has no formal definition but is commonly understood to refer to the underdeveloped, usually (but not only) urban, residential areas that during Apartheid were reserved for non-whites (Africans, Coloureds and Indians) who lived near or worked in areas that were designated 'white only' (under the ...

2.25. "**Youth**" means persons between the ages of 14 and 35 as defined in the National Youth Commission Act of 1996.

3. FORMULAE 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:

80/20 **or** **90/10**

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

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

3.2. FORMULAE 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**

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

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.

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: …… …… …… ……

SBD 7.2 CONTRACT FORM - RENDERING OF SERVICES

THIS FORM MUST BE FILLED IN DUPLICATE BY BOTH THE SERVICE PROVIDER (PART 1) AND THE PURCHASER (PART 2). BOTH FORMS MUST BE SIGNED IN THE ORIGINAL SO THAT THE SERVICE PROVIDER AND THE PURCHASER WOULD BE IN POSSESSION OF ORIGINALLY SIGNED CONTRACTS FOR THEIR RESPECTIVE RECORDS.

PART 1 (TO BE FILLED IN BY THE SERVICE PROVIDER)

1. I hereby undertake to render services described in the attached bidding documents to (name of the institution)……. in accordance with the requirements and task directives / proposals specifications stipulated in Bid Number…….. at the price/s quoted. My offer/s remain binding upon me and open for acceptance by the Purchaser during the validity period indicated and calculated from the closing date of the bid .

2. The following documents shall be deemed to form and be read and construed as part of this agreement:

   (i) Bidding documents, *viz*
   - Invitation to bid;
   - Proof of tax compliance status;
   - Pricing schedule(s);
   - Filled in task directive/proposal;
   - Preference claim form for Preferential Procurement in terms of the Preferential Procurement Regulations;
   - Bidder's Disclosure form;
   - Special Conditions of Contract;

   (ii) General Conditions of Contract; and
   (iii) Other (specify)

3. I confirm that I have satisfied myself as to the correctness and validity of my bid; that the price(s) and rate(s) quoted cover all the services specified in the bidding documents; that the price(s) and rate(s) cover all my obligations and I accept that any mistakes regarding price(s) and rate(s) and calculations will be at my own risk.

4. I accept full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on me under this agreement as the principal liable for the due fulfillment of this contract.

5. I declare that I have no participation in any collusive practices with any bidder or any other person regarding this or any other bid.

6. I confirm that I am duly authorised to sign this contract.

NAME (PRINT) …….

CAPACITY ……

SIGNATURE ……

NAME OF FIRM ……

CONTRACT FORM - RENDERING OF SERVICES

PART 2 (TO BE FILLED IN BY THE PURCHASER)

1. I……. in my capacity as……..……..
accept your bid under reference number ……dated……for the rendering of services indicated hereunder and/or further specified in the annexure(s).

2. An official order indicating service delivery instructions is forthcoming.

3. I undertake to make payment for the services rendered in accordance with the terms and conditions of the contract, within 30 (thirty) days after receipt of an invoice.

DESCRIPTION OF SERVICE	PRICE (ALL APPLICABLE TAXES INCLUDED)	COMPLETION DATE	TOTAL PREFERENCE POINTS CLAIMED	POINTS CLAIMED FOR EACH SPECIFIC GOAL

4. I confirm that I am duly authorised to sign this contract.

SIGNED AT ……ON……..

NAME (PRINT) …….

SIGNATURE …….

OFFICIAL STAMP

WITNESSES

1 ……

2 ……

GOVERNMENT PROCUREMENT

GENERAL CONDITIONS OF CONTRACT
July 2010

NOTES

The purpose of this document is to:

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

To ensure that clients be familiar regarding 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 General Conditions of Contract 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 General Conditions of Contract. Whenever there is a conflict, the provisions in the SCC shall prevail.

TABLE OF CLAUSES

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 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 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 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 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 organization purchasing the goods.

1.22 "Republic" means the Republic of South Africa.

1.23 "SCC" means the Special Conditions of Contract.

1.24 "Services" means those functional services ancillaries 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, special conditions of contract are also laid down to cover specific supplies, services or works.

2.3 Where such special conditions of contract 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.

5. 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:

(a) 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

(b) 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 organization 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 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' 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 the following services, including additional services, if any, specified in SCC:

(a) performance or supervision of on-site assembly and/or Commissioning of the supplied goods.
(b) furnishing of tools required for assembly and/or maintenance of the supplied goods.
(c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods.
(d) performance or supervision or maintenance and/or repair of the supplied goods, for a period agreed by the parties, provided that this service shall not relieve the supplier of any warranty obligations under this contract; and
(e) 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 the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier:

(a) 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
(b) in the event of termination of production of the spare parts:
  (i) Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and
  (ii) 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 authorized 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 canceling 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:

(a) 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.

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

(c) 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:

(i) the name and address of the supplier and / or person restricted by the purchaser.
(ii) the date of commencement of the restriction
(iii) the period of restriction; and
(iv) the reasons for the restriction.

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

23.7 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,

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

(b) the purchaser shall pay the supplier any monies due the supplier.

28. Limitation of Liability

28.1 Except in cases of criminal negligence or willful Misconducts, and in the case of infringement pursuant to Clause 6:

(a) 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

(b) 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.

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 South African Revenue Services.

33. National Industrial Participation (NIP) Programme

33.1 The NIP Programme administered by the Department of Trade and Industry 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.

…… …….....

Signature Date

..... ……

Position Name of bidder

Appendix 08 – Infrastructure Monitoring Service Levels

Appendix 09 – Cybersecurity Service Levels

Appendix 10 – Active Directory Service Levels

Appendix 11 – Storage Systems Service Levels

Section 1.X – Scope Boundaries

UPDATE 1: SCOPE BOUNDARIES
INSERT LOCATION: After Section 1 (Introduction), before Section 2
RENUMBER AS: Section 1.X (adjust X based on your current numbering)
1.X SCOPE BOUNDARIES
1.X.1 IN SCOPE - Service Provider Responsibilities
The service provider is fully responsible for the following:
a) Telecommunications Services:
- Provision of all telecommunications carrier services including voice, data, and internet connectivity
- Partnership with licensed South African telecommunications providers
- End-to-end management of carrier relationships including:
  - Circuit provisioning and activation
  - Fault logging and escalation with carriers
  - SLA management and performance monitoring
  - Billing consolidation and cost optimization
- MS Teams telephony implementation including:
  - Session Border Controllers (SBCs)
  - Direct routing configuration
  - IVR and call centre functionality
  - Number porting coordination
- SD-WAN services with integrated carrier management
- Monthly consolidated billing to CETA for all telecommunications services

NOTE: The service provider must demonstrate an existing partnership or formal agreement with a licensed South African telecommunications carrier. This partnership serves as a quality indicator and ensures proper implementation of unified communications solutions. Joint performance KPIs will be established for telecommunications service delivery.

b) Managed Services Delivery:
- Installation, configuration, and management of all ICT infrastructure
- 24/7/365 monitoring and support for all in-scope services
- Patch management and firmware updates
- Backup and disaster recovery services
- Security monitoring and incident response
- User provisioning and support
- Documentation and knowledge management

c) Project Implementation:
- Standard installations per approved designs
- Configuration of systems per agreed specifications
- User acceptance testing coordination
- Knowledge transfer and training

1.X.2 OUT OF SCOPE - Excluded from Base Service
The following are explicitly excluded from the base managed services contract and will be scoped and priced separately as required:
a) Strategic Planning and Design:
- Initial architecture design for new infrastructure (greenfield)
- Network redesign or major topology changes
- Application architecture and selection
- ICT strategy development

b) Hardware and Software Procurement:
- Capital expenditure for new equipment
- Software license procurement (where not included in service fee)
- Hardware warranty extensions beyond standard OEM terms

NOTE: CETA will establish separate procurement panels for hardware and software. Service provider is responsible for installation, configuration, and ongoing management of procured equipment.

c) Application Development and Customization:
- Custom application development
- Software customization beyond standard configuration
- Integration development (except standard APIs)

d) End-User Training:
- General IT literacy training
- Business application training (except security awareness training which IS in scope)
- Custom training programs

e) Physical Infrastructure:
- Data centre construction or renovation
- Electrical infrastructure (except UPS management)
- Physical cabling installation (except moves/adds/changes to existing infrastructure)
- Physical security systems

f) Ad-Hoc Project Work:
- Major infrastructure upgrades requiring new design
- Migration projects not part of routine operations
- Special projects outside routine managed services

NOTE: Ad-hoc work will be quoted separately at agreed hourly rates as per the pricing schedule.

1.X.3 Grey Areas Requiring Clarification

The following will be clarified during contract negotiation:
- Threshold between "routine change" (in scope) and "project work" (out of scope)
- Hardware refresh responsibility (CETA procures, provider installs?)
- Third-party vendor management scope and authority levels

Section 13 – Transition and Handover Requirements

UPDATE 2: TRANSITION AND HANDOVER REQUIREMENTS
INSERT LOCATION: Create as New Section 13
13. TRANSITION AND HANDOVER REQUIREMENTS
13.1 Transition-In (Contract Commencement)
13.1.1 Transition Planning:
• Detailed transition plan submitted within 10 business days of contract signature
• Plan must include:
  - Transition timeline with milestones (maximum 90-day transition period)
  - Risk assessment and mitigation strategies
  - Communication plan for stakeholders
  - Cutover schedule for each service component
  - Rollback procedures for failed cutover attempts
  - Success criteria for transition completion
• CETA approval required before transition commencement
13.1.2 Knowledge Transfer from Incumbent (if applicable):
• Minimum 30 days overlap with incumbent service provider
• Shadow period where new provider observes current operations
• Access to incumbent's documentation and configurations
• Structured handover sessions covering:
  - Network architecture and topology
  - Active incidents and problems
  - Upcoming changes and projects
  - Known issues and workarounds
  - Vendor contacts and escalation paths
13.1.3 Current State Assessment:
• Comprehensive assessment of CETA's ICT environment within 30 days
• Gap analysis between current state and requirements
• Documented findings including:
  - Infrastructure inventory
  - Configuration audit
  - Security posture assessment
  - Capacity utilization
  - Identified risks and quick wins
• Baseline metrics established for SLA measurement
13.1.4 Parallel Running:
• Minimum 14-day parallel running period for critical services
• Both incumbent and new provider operational simultaneously
• New provider handles increasing percentage of workload:
  - Week 1: 25% of incidents
  - Week 2: 50% of incidents
  - Week 3: 75% of incidents
  - Week 4: 100% cutover
• No service degradation during transition
• Daily status meetings during parallel running
13.1.5 Transition Success Criteria:
• All SLAs met for 14 consecutive days post-cutover
• Zero critical incidents attributable to transition

• All documentation delivered and accepted
• Staff trained on new procedures
• CETA sign-off on transition completion
13.2 Steady-State Operations
13.2.1 Documentation Maintenance:
• All documentation kept current within 48 hours of changes
• Quarterly comprehensive documentation review
• Documents include:
  - Network diagrams (physical, logical, Visio format)
  - Configuration files (backed up and version controlled)
  - Standard operating procedures (SOPs)
  - Runbooks for common incidents
  - Contact lists and escalation matrices
  - Admin credentials (stored in CETA-approved password vault)
13.3 Transition-Out (Contract End or Termination)
13.3.1 Notice Period:
• 90-day notice period for normal contract end
• 30-day notice period available for termination due to non-performance
• Service provider must maintain full service levels throughout notice period
13.3.2 Knowledge Transfer to Successor:
• Minimum 30-day overlap with incoming service provider
• Structured handover sessions (minimum 10 x 2-hour sessions covering):
  - Infrastructure overview and architecture
  - Active incidents and problems
  - Ongoing projects and changes
  - Known issues and workarounds
  - Vendor relationships and escalation procedures
• Shadow period where incoming provider observes operations
• Q&A sessions with CETA staff
13.3.3 Documentation Handover:
• Complete documentation package delivered 30 days before contract end
• Package must include:
  - All network diagrams (current state, validated within 14 days)
  - Complete configuration backups for all devices
  - All scripts, automations, and custom code with source
  - Password vault with all credentials
  - Service history for previous 12 months
  - Contact lists and vendor information
  - Asset inventory with serial numbers and warranty status
• Documentation provided in editable formats (Word, Excel, Visio)
• Digital copies provided on encrypted USB drives (2 copies)
13.3.4 Data and Intellectual Property Return:
• All CETA data returned or securely destroyed within 30 days
• Certificate of data destruction provided for all deleted data
• All CETA-owned licenses transferred at no cost
• All custom developments and IP transferred to CETA
• No retention of CETA data for any purpose
• No ransom of data, credentials, or intellectual property

13.3.5 Access Revocation:
• All service provider access credentials revoked on contract end date
• All VPN access terminated
• All administrator accounts disabled
• All service provider equipment removed from CETA premises within 14 days
• Confirmation of access revocation provided in writing
13.3.6 Final Reconciliation:
• Final invoice submitted within 15 days of contract end
• Any unused prepaid services refunded pro-rata
• Any outstanding liabilities settled
• Performance bond released (if applicable)
• Final service report covering last month of contract
13.3.7 Cooperation Requirements:
• Service provider must fully cooperate with incoming provider
• No obstruction or delay of transition activities
• No poaching of CETA staff for 12 months post-contract
• No negative communication about CETA or successor to vendors

Pricing Schedule – Detailed Requirements

UPDATE 3: DETAILED PRICING SCHEDULE
INSERT LOCATION: Replace existing pricing section (around paragraph 1720)
RENUMBER AS: Maintain existing section number
PRICING SCHEDULE - DETAILED REQUIREMENTS
Bidders must complete the following pricing schedule. All prices must be in South African Rands (ZAR) excluding VAT unless otherwise stated. Prices must remain valid for 180 days from bid submission.
1. MONTHLY RECURRING CHARGES (MRC)
Provide monthly recurring charges for each service category:
SERVICE CATEGORY	MONTHLY FEE (ZAR)	NOTES
1. Service Desk (including system licenses for [X] agents)	
2. IT Service Management	
3. Microsoft Operating Systems ([X] servers)	
4. Wi-Fi and LAN Services ([X] switches, [X] APs)	
5. SD-WAN Services (include carrier costs)		Per site breakdown required
6. Internet Connectivity (200 Mbps 1:1 fully redundant)	
7. Infrastructure Monitoring	
8. Cybersecurity Services (including SOC)	
9. IT Service Delivery (2 x L1 onsite resources)	
10. Unified Communications (MS Teams telephony + MPABX)		Include carrier costs
11. Active Directory Services	
12. Storage Services	
TOTAL MONTHLY RECURRING CHARGE	
1.1 Minimum Contract Period: [specify 36 months]
1.2 Payment Terms: [specify 30 days from invoice date]
1.3 Billing Cycle: Monthly in arrears on last business day of month
2. ONE-TIME IMPLEMENTATION CHARGES (OTC)
IMPLEMENTATION COMPONENT	ONE-TIME FEE (ZAR)	NOTES
Service Desk System Implementation	
Network Infrastructure Audit	
Security Assessment & Baseline	
Migration from Incumbent Provider	
Knowledge Transfer & Training	
Project Management	
Documentation Creation	
TOTAL ONE-TIME IMPLEMENTATION FEE	
3. TELECOMMUNICATIONS CARRIER SERVICES (Included in MRC Above)
Detail the carrier services and costs included in your SD-WAN and Unified Communications pricing:
SITE/SERVICE	CARRIER	SERVICE TYPE	BANDWIDTH	MONTHLY COST	SLA
Head Office - Primary				
Head Office - Secondary				
Eastern Cape				
Free State				

Gauteng (Midrand) | | | | |
KwaZulu-Natal | | | | |
Limpopo | | | | |
Mpumalanga | | | | |
Northern Cape | | | | |
North West | | | | |
Western Cape | | | | |

3.1 Carrier Partnership:
- Name of telecommunications partner: _____
- Nature of partnership (Reseller? Agent? Direct?): _____
- Partnership agreement validity period: _____
- Upload copy of partnership certificate/agreement: _____

3.2 Billing Arrangement:
- Consolidated billing through service provider: YES / NO
- Service provider mark-up on carrier services: _____%
- Carrier SLAs passed through to CETA: YES / NO

3.3 Joint Performance Management:
- Joint KPIs will be established between provider and telco partner
- Monthly performance meetings required with telco participation
- Unified escalation path from CETA → Provider → Telco

4. AD-HOC WORK RATES

Provide hourly rates for work outside routine managed services:

SKILL LEVEL	DESCRIPTION	BUSINESS HOURS	AFTER-HOURS	WEEKEND/HOLIDAY
Level 1 Support	Basic troubleshooting, password resets		
Level 2 Support	Advanced troubleshooting, configuration		
Level 3 Support	Expert-level, design, architecture		
Project Manager	Project work coordination		
Security Specialist	Security assessments, pen testing		

4.1 Minimum Call-Out: ____ hours

4.2 Travel Costs: Included / Separate (specify rate: R____ per km)

4.3 Ad-Hoc Work Approval: All ad-hoc work requires written pre-approval from CETA SM:ICT

5. HARDWARE AND SOFTWARE PROCUREMENT

5.1 Procurement Model:

[ ] CETA procures via separate panels, provider installs/configures (PREFERRED)
[ ] Provider procures on behalf of CETA (specify mark-up: ____%)
[ ] Hybrid (specify which items provider procures): _____

5.2 If provider procures:
- Mark-up percentage on hardware: ____%
- Mark-up percentage on software licenses: ____%
- Payment terms: Net ___ days from delivery
- Warranty management: Provider / OEM Direct / CETA

NOTE: CETA is establishing separate hardware and software procurement panels. Service provider will install, configure, and manage procured equipment.

6. ANNUAL PRICE ESCALATION

6.1 Escalation Mechanism:

[ ] Fixed percentage: ____% per annum
[ ] CPI-linked: South African CPI published by Stats SA

[ ] Hybrid: CPI + ___% or maximum ___% (whichever is lower)
6.2 Escalation Frequency: [ ] Annual on contract anniversary [ ] Other: _____
6.3 First escalation effective date: _____
6.4 Documentation: Price escalation calculations to be submitted annually for approval
7. VOLUME DISCOUNTS AND MULTI-YEAR COMMITMENT
COMMITMENT PERIOD	DISCOUNT OFF TOTAL MRC	NOTES
36 months (minimum)	0% (base price)
48 months	___%
60 months	___%
7.1 Discount Application: Applied to monthly recurring charges only
7.2 Early Termination: If CETA terminates early, discount refunded pro-rata
8. PERFORMANCE INCENTIVES (Optional)
8.1 SLA Performance Bonuses:
- Consistently exceed all SLAs for 12 consecutive months: Bonus of R_____ or ____%
- Zero P1 incidents for 6 consecutive months: Bonus of R_____ or ____%
- Customer satisfaction score >4.5/5.0 for 4 consecutive quarters: Bonus of R_____

8.2 Innovation Incentives:
- Cost savings delivered above ___% threshold: __% of savings shared with provider
- Process improvement implementation: Up to R_____ per approved initiative

9. PAYMENT TERMS AND CONDITIONS
9.1 Invoice Submission: By 5th business day of following month
9.2 Invoice Requirements:
- Itemized breakdown by service category
- Consumption reports attached (bandwidth, storage, licenses)
- Service credit deductions clearly shown
- Any penalties deducted clearly shown

9.3 Payment Terms: Net 30 days from invoice receipt
9.4 Late Payment: Interest at prime rate + 2% per month on overdue amounts
9.5 Disputed Invoices:
- Disputed amounts withheld
- Undisputed amounts paid as normal
- Dispute resolution per Section 14 (Governance)

9.6 Reconciliation: Quarterly reconciliation meetings to review billing accuracy
10. PRICE ADJUSTMENTS FOR SCOPE CHANGES
10.1 Additional Users/Devices:
- Service desk agents: R____ per agent per month
- Servers: R____ per server per month
- Network devices: R____ per device per month
- Endpoints: R____ per endpoint per month
- Cloud services users: R____ per user per month

10.2 Additional Sites:
- New branch office setup fee (OTC): R_____
- Ongoing monthly cost per site: R_____
- Satellite office (< 10 users): R_____ monthly

10.3 Service Level Upgrades:
- Upgrade from 99.9% to 99.99% SLA: Additional ___% of affected service category fee
- 24/7 onsite support vs. remote: Additional R_____ per month per site

10.4 Technology Refreshes:
- Major technology migration project: Quote separately as project work
- Routine upgrade cycles: Included in base service

11. TOTAL CONTRACT VALUE (TCV)

DESCRIPTION	AMOUNT (ZAR)
Total OTC (Implementation)
Total MRC x 36 months
Estimated ad-hoc work (10% of MRC x 36)
TOTAL 3-YEAR CONTRACT VALUE

11.1 Annual Breakdown:
- Year 1 (including OTC): R_____
- Year 2 (with escalation): R_____
- Year 3 (with escalation): R_____

12. FINANCIAL GUARANTEES AND INSURANCE

12.1 Performance Bond:
- Amount: ___% of annual contract value or R_____
- Validity: Duration of contract + 12 months
- Purpose: Guarantee performance obligations

12.2 Professional Indemnity Insurance:
- Minimum coverage: R_____ per incident
- Aggregate coverage: R_____ per annum
- Proof required before contract signature

12.3 Public Liability Insurance:
- Minimum coverage: R_____ per incident
- Required for onsite personnel

PRICING NOTES
- All prices are binding for 180 days from bid submission date
- Prices are exclusive of VAT (VAT will be added at applicable rate)
- Foreign exchange risk (if any): [Specify how managed]
- Price validity subject to no material change in scope
- Hidden costs: Bidders must declare ALL costs - no hidden fees
- Third-party licenses: All third-party license costs must be itemized separately

COST BREAKDOWN REQUIREMENT

For evaluation purposes, bidders must provide detailed cost breakdown showing:
- Personnel costs (onsite staff, SOC analysts, etc.)
- Software licensing costs (per seat/per device)
- Hardware costs (if any)
- Telecommunications carrier costs (itemized by site)
- Overhead and profit margin
- Any subcontractor costs

This breakdown will be treated as commercially confidential.

SLA Performance, Remedies, and Penalties

UPDATE 4: SLA PERFORMANCE, REMEDIES, AND PENALTIES
INSERT LOCATION: New section after requirements, before evaluation criteria
CREATE AS: New Section (suggest numbering after main requirements)
SLA PERFORMANCE, REMEDIES, AND PENALTIES
1. SERVICE LEVEL AGREEMENTS (SLAs)
All service levels are defined in Appendices 01-11. The service provider must meet or exceed all defined SLAs. Performance will be measured monthly and reviewed in monthly service review meetings.
1.1 SLA Categories:
- Availability SLAs (system uptime)
- Response Time SLAs (incident response)
- Resolution Time SLAs (incident resolution)
- Performance SLAs (throughput, latency)
- Quality SLAs (accuracy, completion rates)

2. SLA MEASUREMENT AND REPORTING
2.1 Measurement Period: Calendar month (1st to last day of month)
2.2 Reporting Deadline: Service provider submits SLA report by 2nd Friday of following month
2.3 Report Contents:
- SLA achievement percentage by service category
- Trend analysis (rolling 12-month view)
- Root cause analysis for any breaches
- Corrective actions taken
- Service credits calculation (if applicable)

2.4 Verification: CETA may audit SLA calculations and request supporting evidence
2.5 Dispute Resolution: SLA disputes escalated per Section 14 (Governance), resolved within 10 business days
3. SERVICE CREDITS FOR SLA BREACHES
When the service provider fails to meet an SLA, CETA is entitled to service credits as follows:
3.1 Service Credit Calculation Table:

SLA PERFORMANCE LEVEL	SERVICE CREDIT
95.0% - 99.8% of SLA target	5% of affected service category monthly fee
90.0% - 94.9% of SLA target	10% of affected service category monthly fee
85.0% - 89.9% of SLA target	15% of affected service category monthly fee
Below 85.0% of SLA target	20% of affected service category monthly fee

EXAMPLE CALCULATION:
Cybersecurity service monthly fee: R100,000
SLA target: 99.9% SOC availability
Actual performance: 98.5% (falls in 95.0%-99.8% range)
Service credit: R5,000 (5% of R100,000)
3.2 Service Credit Application:
- Calculated automatically based on monthly performance
- Applied as credit against following month's invoice
- Clearly shown on invoice with calculation methodology
- No dispute required - automatic application

3.3 Service Credit Caps:

• Maximum per service category per month: 20% of that category's monthly fee
• Maximum across all categories per month: 20% of total monthly fee
• No double-counting: If one root cause affects multiple SLAs, credit applied once

3.4 Service Credit Exclusions:

Service credits do NOT apply if SLA breach caused by:
• CETA-requested changes or maintenance
• Force majeure events (defined in main contract)
• Third-party failures outside provider's reasonable control
• CETA's failure to provide required information/approvals
• Planned maintenance approved by CETA

3.5 Cumulative Service Credits:
• Tracked monthly
• If cumulative credits exceed R500,000 in any 12-month period:
→ Triggers Performance Improvement Plan (Section 5)
→ CETA may terminate without penalty

4. CRITICAL INCIDENT PENALTIES (P1 Incidents)

Beyond service credits, specific monetary penalties apply for critical incident response failures:

BREACH TYPE	PENALTY (ZAR)
P1 Incident Response Time breach (>15 minutes)	R10,000 per occurrence
P1 Incident Resolution Initiation breach (>1 hour)	R25,000 per occurrence
P1 Security Incident Response breach (>15 minutes)	R15,000 per occurrence
Data breach due to provider negligence	R100,000 + actual damages
Unauthorized access due to provider error	R50,000 per occurrence
Failed backup discovery	R25,000 per occurrence
Unplanned downtime >4 hours	R50,000 per day
SLA reporting failure (not submitted by deadline)	R5,000 per day late

4.1 Penalty Payment Process:
• Provider notified in writing of breach and penalty
• Provider has 5 business days to dispute with evidence
• If undisputed or dispute rejected:
→ Penalty invoiced separately
→ Payment due within 15 days
→ May be offset against provider invoices

4.2 Penalty Caps:
• Maximum penalties per calendar quarter: R250,000
• Maximum penalties per calendar year: R500,000
• Penalties above caps trigger contract review

4.3 Relationship to Service Credits:
• Penalties are in addition to service credits
• Example: P1 incident response breach triggers both:
→ R10,000 penalty (immediate)
→ Service credit if monthly SLA missed (month-end)

5. PERSISTENT NON-PERFORMANCE

5.1 Performance Improvement Plan (PIP)

PIP TRIGGER CONDITIONS:
• Any single SLA below target for 3 consecutive months, OR

• Multiple SLAs (3+) below target for 2 consecutive months, OR
• Cumulative service credits exceed R250,000 in any 6-month period
PIP REQUIREMENTS:
• Provider submits PIP within 10 business days of trigger
• PIP must include:
  - Root cause analysis (5 Whys or equivalent)
  - Corrective actions with timelines
  - Preventive measures to avoid recurrence
  - Weekly progress reporting
  - Success criteria for PIP closure
• CETA approval required before PIP implementation
• Monthly progress reviews with CETA SM:ICT
• PIP costs borne entirely by service provider
• PIP period: Maximum 90 days to restore performance
PIP MONITORING:
• Weekly status reports to CETA SM:ICT
• Bi-weekly review meetings
• Immediate escalation if PIP not tracking to plan
5.2 Material Breach and Termination Rights
CETA may terminate contract without penalty if:
IMMEDIATE TERMINATION TRIGGERS:
• Wilful misconduct or fraud by provider
• Unauthorized access to CETA data
• Data breach due to gross negligence
• Provider bankruptcy or insolvency
• Loss of required certifications (e.g., telco partnership)
TERMINATION AFTER NOTICE/CURE PERIOD:
• Any SLA below 85% for 6 consecutive months, OR
• Multiple SLAs (3+) below target for 6 consecutive months, OR
• Total service credits exceed R500,000 in any 12-month period, OR
• Five or more P1 incident response breaches in any calendar quarter, OR
• Provider fails to implement approved PIP within 90 days, OR
• Repeated material policy violations (3+ in 12 months)
TERMINATION PROCESS:
• CETA provides written notice specifying breach
• Provider has 30 days to cure (if curable)
• If not cured: CETA may terminate with 30 days notice
• Transition-out process per Section 13 commences immediately
CONSEQUENCES OF PROVIDER-FAULT TERMINATION:
• Service provider liable for:
  - Transition-out costs
  - CETA's re-procurement costs (up to R500,000)
  - Outstanding service credits and penalties
  - Any incremental costs CETA incurs with replacement provider for first 6 months
• Performance bond forfeited
• No refund of implementation fees
6. PERFORMANCE BONUSES (Incentive Structure)
To incentivize exceptional performance, CETA may award performance bonuses:

BONUS CRITERIA	BONUS AMOUNT
All SLAs met or exceeded for 12 consecutive months	2% of annual contract value OR R_____ (whichever is lower)
Zero P1 incidents for 12 consecutive months	R_____
Customer satisfaction score ≥4.5/5.0 for 4 consecutive quarters	R_____
Cost savings delivered exceeding agreed threshold	__% of savings amount (define threshold)
Innovation award (by CETA discretion)	Up to R_____

6.1 Bonus Eligibility:
- Provider must have no outstanding service credits or penalties
- Provider must have no open PIPs
- Provider must be current on all contractual obligations
- Bonuses not guaranteed - awarded at CETA discretion

6.2 Bonus Payment:
- Calculated and paid quarterly in arrears
- Paid via credit on quarterly invoice
- Subject to availability of CETA budget

6.3 Innovation Bonus Details:
- Provider proposes innovation/improvement
- CETA evaluates business case
- If approved and implemented, bonus calculated based on verified savings
- Savings verified by CETA Finance for 6 months post-implementation

7. SLA REVIEW AND ADJUSTMENT

7.1 Annual SLA Review:
- Conducted in Annual Strategic Planning Session
- Both parties may propose SLA adjustments
- Must be mutually agreed and formally documented
- Adjusted SLAs effective from next contract anniversary

7.2 Technology-Driven Adjustments:
- If new technology enables better performance, SLAs may be tightened
- If technology refresh required for SLA, costs shared or CETA procures

7.3 Baseline Reset:
- After 12 months, performance baselines may be reset
- Based on demonstrated capability
- Cannot reduce below original RFP requirements

8. REPORTING AND TRANSPARENCY

8.1 Real-Time SLA Dashboard:
- Provider must provide web-based SLA dashboard
- Updated hourly (minimum)
- CETA SM:ICT read-only access
- Shows current month-to-date performance

8.2 Monthly SLA Report Components:
- Executive summary (1-page)
- SLA achievement by service category
- Trend charts (12-month rolling)
- Root cause analysis for breaches
- Corrective actions and status
- Service credits and penalties summary

- Forecast for next month

8.3 Quarterly SLA Deep Dive:
- Presented in Quarterly Business Review
- Includes year-over-year comparison
- Identifies improvement opportunities
- Forecasts for next quarter

8.4 Audit Rights:
- CETA may audit SLA data and calculations quarterly
- 5 business days notice (or immediate for cause)
- Provider must provide:
  - Raw monitoring data
  - Incident tickets and timestamps
  - Change logs
  - Any other supporting evidence
- Audit costs borne by CETA unless material discrepancies found

9. DISPUTE RESOLUTION FOR SLA DISAGREEMENTS

9.1 Level 1 - Technical Discussion:
- Provider Service Manager and CETA SM:ICT
- Response: 5 business days
- 80% of disputes resolved here

9.2 Level 2 - Management Escalation:
- Provider Account Director and CETA CIO
- Response: 10 business days
- Independent technical review if needed (costs shared)

9.3 Level 3 - Executive Escalation:
- Provider Executive and CETA CEO
- Response: 15 business days
- May engage independent arbitrator (costs shared)

9.4 Interim Measures:
- Disputed service credits held in escrow
- Undisputed amounts paid as normal
- Service delivery continues unaffected
- SLA measurement and reporting continues

10. FORCE MAJEURE AND SLA RELIEF

10.1 Force Majeure Events:
- Natural disasters (flood, earthquake, fire)
- War, terrorism, civil unrest
- Government action (excluding licensing/regulatory compliance)
- Strikes (excluding provider's own employees)
- Pandemics declared by WHO

10.2 SLA Relief Process:
- Provider notifies CETA immediately
- Provides evidence of force majeure
- Proposes mitigation measures
- CETA evaluates and approves/denies
- SLA relief granted only for period and scope affected

10.3 Provider Obligations During Force Majeure:
- Implement business continuity plan

- Provide regular updates (daily)
- Minimize service impact
- Resume normal service ASAP
- No service credits during approved force majeure period

Data Protection and Compliance
UPDATE 5: DATA PROTECTION, PRIVACY, AND COMPLIANCE
INSERT LOCATION: New section (suggest after Section 10 or as Section 15)
CREATE AS: New Section with comprehensive subsections
DATA PROTECTION, PRIVACY, AND COMPLIANCE
1. LEGAL AND REGULATORY FRAMEWORK
1.1 Protection of Personal Information Act (POPI Act, 2013):
ROLES AND RESPONSIBILITIES:
• CETA: Responsible Party (retains ultimate accountability)
• Service Provider: Operator (processes data on CETA's instructions)
• Relationship: Principal-Agent for data protection purposes
CONTRACTUAL REQUIREMENTS:
• Data Processing Agreement (DPA) must be executed before contract commencement
• DPA must comply with POPI Act Section 21 and Chapter 9
• Provider bound by CETA's data protection policies
• Provider may only process personal information per CETA written instructions
1.2 Other Applicable South African Legislation:
• Electronic Communications and Transactions Act (ECTA), 25 of 2002
• Regulation of Interception of Communications Act (RICA), 70 of 2002
• Promotion of Access to Information Act (PAIA), 2 of 2000
• Cybercrimes Act, 19 of 2020
• National Cybersecurity Policy Framework (2015)
• King IV Corporate Governance Code
• Public Finance Management Act (PFMA) - as CETA is public entity
1.3 International Standards (for reference):
• ISO/IEC 27001:2013 - Information Security Management
• ISO/IEC 27701:2019 - Privacy Information Management
• NIST Cybersecurity Framework
• CIS Controls v8
2. DATA SOVEREIGNTY AND RESIDENCY
2.1 Geographic Restrictions (MANDATORY):
ALL CETA DATA MUST REMAIN IN SOUTH AFRICA:
• Primary storage: South African data centres only
• Backup storage: South African data centres only
• Disaster recovery: South African data centres only
• Processing: All data processing within South African borders
• No offshore access: No remote access from outside South Africa
2.2 Approved Cloud Service Regions:
IF CLOUD SERVICES USED:
• Microsoft Azure: South Africa North (Johannesburg) OR South Africa West (Cape Town)
• Amazon AWS: Africa (Cape Town) region only
• Google Cloud: Not yet available in SA - not permitted until local region available
• Other providers: Must have physical data centres in South Africa
VERIFICATION REQUIRED:

• Provider must provide data centre location certificates
• Annual attestation of data residency compliance
• Right to audit data centre locations
2.3 Cross-Border Data Transfer Restrictions:
GENERAL PROHIBITION:
• No cross-border transfer of CETA data without specific written approval
• Approval required from CETA CIO + Legal Counsel
EXCEPTIONAL CIRCUMSTANCES (if approved):
• Must comply with POPI Act Chapter 9 (Transborder Information Flows)
• Destination country must have adequate level of protection OR
• Standard Contractual Clauses (SCC) must be executed
• Data transfer impact assessment required
• Limited to specific data elements and purpose
• Time-bound approval (reviewed annually)
2.4 Remote Support Restrictions:
SOUTH AFRICAN SUPPORT ONLY:
• All support staff must be South African citizens or permanent residents
• All support must be delivered from within South Africa
• No remote desktop connections from outside South Africa
• VPN connections geo-fenced to South African IP ranges
OEM VENDOR SUPPORT EXCEPTION:
• Original Equipment Manufacturer support may be international
• BUT: OEM must not access CETA data directly
• Provider remains intermediary for OEM support
• Screen sharing monitored and recorded
• CETA data anonymized before sharing with international OEM
3. DATA PROTECTION OBLIGATIONS
3.1 Data Classification and Handling:
ALL CETA DATA CLASSIFIED AS CONFIDENTIAL (minimum):
• Public: Information already in public domain
• Internal: General business information
• Confidential: Most CETA information (default)
• Restricted: Personal information, financial data
• Highly Restricted: Credentials, encryption keys
HANDLING REQUIREMENTS PER CLASSIFICATION:
• Confidential and above: Encrypted at rest and in transit
• Restricted and above: Access logged and monitored
• Highly Restricted: Multi-factor authentication required
3.2 Confidentiality Requirements:
NON-DISCLOSURE OBLIGATIONS:
• All provider staff sign NDAs before accessing CETA data
• NDAs survive contract termination (perpetual confidentiality)
• Subcontractors bound by same confidentiality terms
• No disclosure to third parties without written CETA consent
ACCESS CONTROL:
• Need-to-know basis only
• Role-based access control (RBAC)
• Principle of least privilege

• Quarterly access reviews and certifications
3.3 Security Measures (Mandatory):
ENCRYPTION REQUIREMENTS:
• Data at rest: AES-256 or equivalent approved algorithm
• Data in transit: TLS 1.2 minimum, TLS 1.3 preferred
• Encryption key management:
  - Keys stored separately from encrypted data
  - Key rotation every 12 months minimum
  - CETA retains master keys or key escrow
AUTHENTICATION AND ACCESS:
• Multi-factor authentication (MFA) for ALL administrative access
• Strong password policy (min 12 characters, complexity rules)
• Session timeouts (15 minutes inactivity for admin, 30 for users)
• No shared accounts - individual accountability
MONITORING AND LOGGING:
• All data access logged (who, what, when, where, why)
• Logs retained 12 months minimum
• Real-time alerting on suspicious activity
• Logs tamper-proof (WORM or equivalent)
NETWORK SECURITY:
• Network segmentation (CETA data isolated)
• Intrusion Detection/Prevention Systems (IDS/IPS)
• Firewalls with deny-by-default rules
• Regular vulnerability scanning and patching
3.4 Data Minimization:
COLLECT ONLY WHAT'S NECESSARY:
• Provider collects/processes only data required for service delivery
• No use of CETA data for provider's own purposes
• No data mining or analytics without explicit written consent
• No use of CETA data for training AI/ML models
DATA RETENTION LIMITS:
• Operational data: Retained only as long as required for service delivery
• Backups: Per agreed backup retention policy
• Logs: 12 months (unless longer required by law)
• Upon contract end: All data deleted per Section 7
4. DATA BREACH MANAGEMENT
4.1 Data Breach Definition:
A DATA BREACH INCLUDES ANY OF:
• Unauthorized access to CETA systems or data
• Unauthorized disclosure of CETA data (internal or external)
• Loss or theft of data or devices containing CETA data
• Ransomware or malware affecting CETA data integrity
• Accidental deletion or corruption of CETA data
• Unauthorized modification of CETA data
• Insider threat (malicious or accidental)
4.2 Breach Notification Timeline (MANDATORY):
EVENT	TIMELINE	ACTION REQUIRED

Provider discovers potential breach | Immediate | Internal escalation to provider security team
Breach confirmed | Within 1 hour | Notify CETA SM:ICT verbally
Breach assessment complete | Within 4 hours | Notify CETA SM:ICT in writing (email acceptable)
Executive notification | Within 8 hours | Provider notifies CETA CIO and CEO
Information Regulator notification (if personal data) | Within 72 hours | Joint notification (provider drafts, CETA approves)
Affected data subjects notification (if required) | As determined | Per POPI Act guidance and CETA legal advice

NOTIFICATION MUST INCLUDE:
• Nature and extent of breach
• Data categories and number of records affected
• Individuals affected (if personal information)
• Likely consequences
• Measures taken to mitigate
• Contact person for further information

4.3 Breach Response Requirements:

IMMEDIATE ACTIONS (within 1 hour of detection):
• Contain breach (isolate affected systems)
• Preserve evidence (snapshots, logs)
• Activate incident response team
• Notify CETA per timeline above

SHORT-TERM ACTIONS (within 24 hours):
• Begin forensic investigation
• Assess scope and impact
• Implement additional controls if needed
• Provide CETA with preliminary assessment

MEDIUM-TERM ACTIONS (within 5 business days):
• Complete forensic investigation
• Provide CETA with detailed breach report:
  - Timeline of events (minute-by-minute)
  - Root cause analysis
  - Data affected (classification, volume, sensitivity)
  - Individuals affected (if personal information)
  - Technical details of vulnerability exploited
  - Remediation actions taken
  - Preventive measures implemented
• Lessons learned documented

4.4 Breach Liability and Financial Responsibility:

PROVIDER LIABLE IF BREACH CAUSED BY:
• Provider negligence or failure to follow security policies
• Provider failure to implement required security controls
• Provider employee misconduct
• Provider subcontractor failure
• Inadequate provider security practices

PROVIDER FINANCIAL OBLIGATIONS:
• All breach response costs (forensics, legal, notifications)
• Credit monitoring services if financial/ID data breached (2 years minimum)
• Regulatory fines imposed by Information Regulator (if breach due to provider fault)

• Legal costs if data subjects pursue claims
• Reputational damage to CETA (up to agreed cap)
• Cost to restore data from backups
BREACH PENALTY (in addition to costs above):
• Provider negligence causing breach: R100,000 per breach
• Gross negligence: R250,000 per breach
• Wilful misconduct: R500,000 + termination rights
INSURANCE REQUIREMENT:
• Provider must maintain cyber liability insurance covering:
  - First-party costs (response, recovery)
  - Third-party claims (data subjects, regulators)
  - Minimum coverage: R50 million per incident
  - Aggregate coverage: R100 million per annum
5. COMPLIANCE MONITORING AND REPORTING
5.1 Real-Time Compliance Dashboard:
PROVIDER MUST PROVIDE WEB-BASED DASHBOARD WITH:
• Compliance status against ISO27001:2013 controls
• Compliance status against POPI Act requirements (8 conditions)
• Compliance status against CIS Controls v8
• Open compliance gaps with severity ratings
• Remediation progress and target dates
• Upcoming compliance activities
DASHBOARD REQUIREMENTS:
• Updated daily (minimum)
• CETA SM:ICT and CIO read-only access
• 99.9% dashboard availability
• Historical trending (12 months)
5.2 Monthly Compliance Reporting:
MONTHLY REPORT DUE: 2nd Friday of following month
REPORT MUST INCLUDE:
• Executive summary (1 page)
• Compliance scorecard (% compliant per framework)
• New compliance gaps identified
• Remediation progress on open gaps
• Upcoming compliance activities (next 90 days)
• Changes to regulatory landscape
• Recommendations for CETA
5.3 Quarterly Compliance Deep Dive:
PRESENTED IN QUARTERLY BUSINESS REVIEW:
• Detailed compliance posture assessment
• Gap analysis and remediation roadmap
• Regulatory changes impact analysis
• Third-party audit results (if any)
• Compliance training completion rates
• Security incidents related to non-compliance
5.4 Annual Compliance Attestation:
PROVIDER EXECUTIVE ATTESTATION (CEO or CIO):
• Signed annual letter confirming:

- Full POPI Act compliance
- ISO27001 compliance (if certified)
- All CETA data protected per contract requirements
- No data breaches unreported to CETA
- All subcontractors compliant
- Insurance policies current

• Letter submitted 30 days before contract anniversary
• Failure to provide: Contract suspension until provided

6. AUDIT RIGHTS

6.1 CETA Internal Audit Rights:

CETA MAY AUDIT PROVIDER AT ANY TIME:

• Frequency: Quarterly scheduled + ad-hoc for cause
• Notice: 5 business days advance notice (or immediate for cause)
• Scope: All systems, processes, and facilities handling CETA data
• Access: Full access to documentation, systems, personnel
• Costs: CETA bears costs unless audit reveals material non-compliance

AUDIT DELIVERABLES:

• Audit report within 15 business days
• Findings categorized (Critical, High, Medium, Low)
• Provider response and remediation plan (10 business days)
• Follow-up audit to verify remediation (provider cost if non-compliance found)

6.2 Third-Party Audit Rights:

CETA MAY ENGAGE EXTERNAL AUDITORS:

• Independent third-party security assessors
• Penetration testers
• Compliance auditors (ISO27001, POPI Act)

PROVIDER OBLIGATIONS:

• Full cooperation with third-party auditors
• Auditors sign NDAs before engagement
• Provider provides requested evidence/access
• CETA shares audit reports with provider
• Costs borne by CETA (unless material non-compliance found)

6.3 Regulatory Audit Rights:

IF INFORMATION REGULATOR OR OTHER REGULATOR AUDITS PROVIDER:

• Provider must notify CETA within 24 hours
• CETA may participate in regulatory audit
• Provider provides CETA with copy of:
  - Audit notification letter
  - All submissions to regulator
  - Draft and final audit reports
• Provider must remediate findings within regulator's timelines
• Provider keeps CETA informed of remediation progress

7. DATA RETENTION AND DESTRUCTION

7.1 Data Retention During Contract:

OPERATIONAL DATA:

• Retained as long as required for service delivery
• No arbitrary deletion without CETA approval

BACKUP DATA:

• Retention per agreed backup policy (suggest 90 days online)
• Long-term archives (if any) per CETA's retention schedule
AUDIT LOGS:
• 12 months minimum (online and searchable)
• 24 months archived (retrievable within 48 hours)
EMAIL AND COMMUNICATIONS:
• Per CETA's email retention policy (to be provided)
• Financial-related: 7 years minimum
7.2 Data Destruction Upon Contract End:
PROVIDER OBLIGATIONS WITHIN 30 DAYS OF CONTRACT END:
• Return all CETA data in usable formats, OR
• Securely destroy all CETA data
DATA RETURN OPTION:
• Formats: Native formats, CSV, SQL dump, etc. (CETA specifies)
• Media: Encrypted USB drives or secure cloud transfer
• Verification: CETA tests data integrity before destruction
SECURE DESTRUCTION OPTION:
• Method: NIST 800-88 or equivalent (crypto-erase, overwrite, physical destruction)
• Scope: All copies, including:
  - Production systems
  - Backup systems
  - Disaster recovery systems
  - Test/development systems
  - Employee devices
  - Subcontractor systems
• Certificate of Destruction:
  - Provided within 45 days
  - Signed by provider executive
  - Lists all systems/media destroyed
  - Confirms destruction method used
7.3 Device and Media Disposal:
HARDWARE CONTAINING CETA DATA MUST BE SANITIZED:
• Before disposal, redeployment, or return
• Method: NIST 800-88 Rev. 1 compliant
  - Hard drives: Crypto-erase or physical destruction
  - SSDs: Crypto-erase (overwrite insufficient)
  - Tapes: Degaussing or physical destruction
DISPOSAL CERTIFICATES:
• Certificate for each device disposed
• Includes: Asset tag, serial number, destruction date, method
• Retained by both parties for 7 years
8. SUBCONTRACTING AND THIRD-PARTY ACCESS
8.1 Subcontractor Approval:
ALL SUBCONTRACTORS REQUIRE PRE-APPROVAL:
• Written request to CETA describing subcontractor role
• Subcontractor compliance documentation provided:
  - Security certifications (ISO27001, etc.)
  - POPI Act compliance attestation

- Insurance certificates
- Company registration documents

• CETA approval within 15 business days
• Approval valid for contract duration (or shorter if specified)

SUBCONTRACTOR OBLIGATIONS:
• Same data protection standards as prime provider
• Sign Data Processing Agreement with provider
• Provider remains liable for subcontractor breaches
• CETA audit rights extend to subcontractors

8.2 Third-Party Access Log:

PROVIDER MAINTAINS REGISTER OF ALL THIRD PARTIES WITH CETA DATA ACCESS:
• Party name and company
• Access granted date
• Access revoked date
• Purpose of access
• Data accessed (types and volumes)
• Approval authority

LOG PROVIDED TO CETA:
• Quarterly (with quarterly report)
• Upon request (within 48 hours)
• Includes current AND historical access (full contract duration)

9. DATA PORTABILITY AND EXPORT

9.1 Data Export Rights (During Contract):

CETA MAY REQUEST DATA EXPORT AT ANY TIME:
• Purpose: Backup, audit, analysis, migration preparation
• Frequency: Up to 2 requests per year at no charge
• Additional requests: Charged at agreed hourly rate

EXPORT FORMATS:
• Databases: SQL dumps, CSV, or native format
• Files: Native formats, organized folder structure
• Configurations: Text, JSON, or XML
• Delivery: Encrypted USB, secure file transfer, or cloud storage

DELIVERY TIMELINE:
• Standard request: 10 business days
• Urgent request: 5 business days (surcharge may apply)

9.2 Data Migration Support:

UPON CONTRACT END, PROVIDER MUST ASSIST DATA MIGRATION:
• Full data export in usable formats
• Schema documentation provided
• Migration support:
  - 40 hours included (no charge)
  - Additional hours at agreed rate or included in transition-out
• Testing and validation assistance
• Coordination with successor provider

10. PRIVACY IMPACT ASSESSMENTS (PIAs)

10.1 Initial PIA:

PROVIDER CONDUCTS PIA BEFORE SERVICE COMMENCEMENT:
• Assess privacy risks of proposed service delivery model

• Identify personal information to be processed
• Evaluate necessity and proportionality
• Identify risks to data subject rights
• Propose mitigation measures
PIA SUBMITTED TO CETA FOR APPROVAL:
• Within 20 business days of contract signature
• CETA reviews and approves/requests changes
• Service delivery begins only after PIA approved
10.2 Ongoing PIAs:
CONDUCT NEW PIA WHEN:
• Significant service changes
• New technologies introduced
• New subcontractors engaged
• Material increase in data processing volume/scope
• Regulatory changes affecting privacy
TIMELINE:
• PIA completed BEFORE implementing change
• Submitted to CETA for approval
• Change proceeds only after PIA approved
11. DATA SUBJECT RIGHTS
11.1 Supporting CETA's Data Subject Rights Obligations:
CETA AS RESPONSIBLE PARTY MUST HONOR DATA SUBJECT RIGHTS:
• Right to access personal information
• Right to correction
• Right to deletion (right to be forgotten)
• Right to object to processing
• Right to data portability
PROVIDER'S SUPPORT OBLIGATIONS:
• Assist CETA in responding to data subject requests
• Response within 5 business days of CETA request
• Provide data extracts, correction capability, deletion confirmation
• No charge for first 10 requests per year
• Reasonable fees for additional requests
11.2 Data Subject Request Process:
CETA RECEIVES REQUEST → CETA FORWARDS TO PROVIDER → PROVIDER RESPONDS
Timeline: 21 days (per POPI Act) for CETA to respond to data subject
Therefore: Provider must respond to CETA within 5 business days
PROVIDER MUST PROVIDE:
• Complete data for that data subject
• Source of data
• Processing purpose
• Third parties data shared with
• Retention period
12. TRAINING AND AWARENESS
12.1 Provider Staff Training:
MANDATORY TRAINING FOR ALL PROVIDER STAFF WITH CETA DATA ACCESS:
• POPI Act fundamentals (before access granted)
• CETA's data protection policies (before access granted)

• Information security awareness (annual refresh)
• Incident response procedures (annual refresh)
TRAINING RECORDS:
• Provider maintains training records (course, date, attendee)
• Provided to CETA quarterly
• CETA may audit training completion
12.2 CETA Staff Training Support:
PROVIDER ASSISTS WITH CETA'S DATA PROTECTION TRAINING:
• Provide subject matter experts for training sessions
• Develop training materials (if requested)
• Deliver training to CETA staff (if requested)
• Contribute to CETA's privacy awareness campaigns
13. EMERGING TECHNOLOGIES AND RISKS
13.1 Artificial Intelligence and Machine Learning:
IF AI/ML USED FOR CETA SERVICE DELIVERY:
• Provider must disclose use of AI/ML
• Provide transparency on:
  - What AI/ML is used for
  - Data used to train models
  - Decision-making logic (to extent possible)
  - Accuracy and bias testing results
• CETA retains right to opt-out of AI-based processing
• No use of CETA data to train general-purpose AI models
13.2 Quantum Computing Risks:
PROVIDER MONITORS QUANTUM COMPUTING DEVELOPMENTS:
• Quantum computers may break current encryption
• Provider tracks "quantum readiness"
• Migration plan to quantum-resistant cryptography
• Presented in annual strategic planning session
13.3 New Privacy Regulations:
PROVIDER MONITORS REGULATORY LANDSCAPE:
• Inform CETA of new/changing regulations
• Assess impact on service delivery
• Propose compliance roadmap
• Implement changes (costs shared if material scope change)