TERMS OF REFERENCE

NT013-2026

APPOINTMENT OF A SERVICE PROVIDER FOR THE PROCUREMENT OF THE BACKUP SOLUTION FOR NATIONAL TREASURY FOR A PERIOD OF FIVE (5) YEARS

NON-COMPULSORY VIRTUAL BRIEFING SESSION TO BE HELD:

13 NOVEMBER 2026 (MICROSOFT TEAMS)

CLOSING DATE AND TIME OF BID

30 NOVEMBER 2026 AT 11H00

BID VALIDITY PERIOD:

90 DAYS

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

A NATION THAT WORKS

2030 NDP

CONTENTS

SECTION A: INTRODUCTION AND TERMS OF REFERENCE 7
1. DESCRIPTION AND FORMAT OF THE BID 7
2. LEGISLATIVE AND REGULATORY FRAMEWORK 7
3. DURATION OF CONTRACT 7
4. BRIEFING SESSION 7
5. TERMS OF REFERENCE 8
SECTION B: CONDITIONS OF BID 23
6. PART 1: EVALUATION CRITERIA 23
PART 2: ADDITIONAL BID REQUIREMENTS 35
7. TERMS AND CONDITIONS 35
8. THIRD PARTY AGREEMENTS AND SUB-CONTRACTOR AGREEMENTS 36
9. SUBMISSION OF BIDS 36
10. COMMUNICATION AND CONFIDENTIALITY 36
11. CONTACT DETAILS 37
12. PART 3: RECOMMENDATION AND APPOINTMENT OF BIDDERS 37

LIST OF TABLES

Table 1: Bid Document Checklist and Returnable 8
Table 2: Summary of Technical Specification.
Table 3: Evaluation Criteria 34
Table 4: Functionality Evaluation 38
Table 5: Preference Point System 42

ANNEXURES

Annexure A	:	General Conditions of Contract (GCC)
Annexure B	:	Standard Bidding Documents (SBD's)
Annexure C	:	Pricing Schedule
Annexure D	:	Guide for online bid submission
Annexure E	:	Mandatory Functional Requirements Tables

LIST OF ABBREVIATIONS

ABBREVIATION	FULL NAME
BAC	Bid Adjudication Committee
BEC	Bid Evaluation Committee
B-BBEE	Broad-Based Black Economic Empowerment
CIPC	Companies and Intellectual Property Commission
CSD	Central Supplier Database
NT	National Treasury
PPR 2022	Preferential Procurement Regulation 2022
QSE	Qualified Small Enterprise
RSA	Republic of South Africa
SLA	Service Level Agreement
SARS	South African Revenue Service
SCC	Special Conditions of Contract
SBD	Standard Bidding Document
VAT	Value Added Tax

DEFINITIONS

Name	Definition
Customer	A participant on the contract who procures goods and/or services from the appointed Supplier(s).
Delivery	The process of transporting goods from a bidder's source location to a predefined destination by the participants.
Due Diligence	The investigation or exercise of care that the State conducts before entering into an agreement with the bidders to validate the bid responses.
ITOM	IT Operations Management
SIEM	Security Information and Event Management.
NAS	Network Attached Storage
IoC	Indicator of Compromise.
RBAC	Role-Based Access Control
D2D2C	Disk-to-Disk-to-Cloud backup architecture.
GV	Governance.
IaaS	Infrastructure as a Service.
RDBMS	Relational Database Management System.

TABLE 1: BID DOCUMENT CHECKLIST AND RETURNABLE

#	Document Name	Included in the published bid document?	To be returned by bidder?	Bidder to tick Yes if document is submitted
PHASE 1: MANDATORY REQUIREMENTS				
SBD 3.3 Pricing Schedule		Yes	Yes	
Mandatory Functional Requirements		Yes	Yes	
PHASE 2: LEGISLATIVE AND OTHER STANDARD BIDDING REQUIREMENTS				
1.	SBD 1 Invitation form to bid	Yes	Yes	
2.	SBD 4 Declaration of Interest	Yes	Yes	
3.	SBD 6.1 Preference Points Claim Form	Yes	Yes	
4.	Full CSD report	No	Yes	
5.	CIPC documents	No	Yes	
6.	CV template	Yes	Yes	
7.	Copies of qualifications	No	Yes	
8.	Signed teaming agreement	No	If Applicable	
9.	Valid Tax Clearance Certificate and/or SARS-issued pin code	No	Yes	
10.	Consolidated Central Supplier Database Registration (CSD) full report in the case of a joint venture	No	If Applicable	
PHASE 3: FUNCTIONALITY				
	Bidder must submit supporting documents. Minimum threshold of 70 % must be achieved	No	Yes	
PHASE 4: ONLINE PRESENTATION				
	Minimum threshold of 70 % must be achieved	No	Yes	
PHASE 5: PRICE & SPECIFIC GOALS				
	Proof of specific goals requirements	No	Yes	

SECTION A: INTRODUCTION AND TERMS OF REFERENCE

1. DESCRIPTION AND FORMAT OF THE BID

1.1. This bid is for the appointment of a suitably qualified service provider for the supply, delivery, installation, configuration, commissioning, and support of an enterprise backup and recovery solution, including the provision of all required hardware, software licenses, maintenance, and technical support services. The successful bidder will be required to enter a five (5) year Service Level Agreement (SLA) with the National Treasury for ongoing maintenance, support, software updates, and operational assistance to ensure the continued availability, reliability, security, and performance of the backup solution.

1.2. The solution shall provide secure data protection across the Primary Data Centre, High Availability (HA) Site, and Cloud Archive Repository while ensuring compliance with government information security requirements and business continuity objectives.

1.3. This bid document is structured as follows:

- Section A : Introduction and Terms of Reference
- Section B : Conditions of Bid
- Part 1 : Evaluation Criteria
- Part 2 : Additional Bid Requirements
- Part 3 : Recommendation and Appointment of Bidders
- Section C : Conditions of Contract

2. LEGISLATIVE AND REGULATORY FRAMEWORK

2.1. This bid and all contracts emanating therefrom will be subject to the General Conditions of Contract issued in accordance with Treasury Regulation 16A, published in terms of the Public Finance Management Act, 1999 (Act 1 of 1999) (PFMA), as well as the Preferential Procurement Policy Framework Act, 2000 (PPPFA), with its latest 2022 regulations.

2.2. The Special Conditions of Contract (SCC) are supplementary to the General Conditions of Contract (GCC). However, where the Special Conditions of Contract conflict with the General Conditions of Contract, the Special Conditions of Contract prevail.

3. DURATION OF CONTRACT

3.1. The Contract shall be for a period of five (5) years.

4. BRIEFING SESSION

4.1. A non-compulsory virtual briefing session will be held as follows:

Venue : TEAMS
Date : 13 November 2026
Link : https://teams.microsoft.com/meet/3861824924209451?p=h1ue0fRvL5aEdb2qxi
Time : 10:00 am

4.2. The bid information session is not compulsory but will provide bidders with an opportunity to obtain clarity on certain aspects of the procurement process as set out in this bid document.

4.3. The National Treasury reserves the right to answer questions at the briefing session and/or to respond formally after the briefing session.

5. TERMS OF REFERENCE

5.1. Technical Specifications

5.1.1. This bid is for the appointment of a suitably qualified service provider for the supply, delivery, installation, configuration, commissioning, and support of an enterprise backup and recovery solution, including the provision of all required hardware, software licenses, maintenance, and technical support services. The successful bidder will be required to enter a five (5) year Service Level Agreement (SLA) with the National Treasury for ongoing maintenance, support, software updates, and operational assistance to ensure the continued availability, reliability, security, and performance of the backup solution.

5.1.2. The scope of work entails the procurement and implementation of a comprehensive Cyber Resilience and Data Protection Solution for National Treasury. The solution will provide secure backup, recovery, replication, and cyber resilience capabilities for data stored across on-premises infrastructure, including physical and virtual servers, applications, databases, Microsoft 365 workloads, and identity systems.

5.1.3. Recognising backup as the critical last line of defence against data loss, corruption, system failures, and malicious attacks, the solution must enable reliable data recovery, support disaster recovery (DR) operations, and facilitate the replication of data between the Production and Disaster Recovery sites. While backup forms an essential component of the DR strategy, its role will be guided by National Treasury's Business Impact Analysis (BIA) and broader business continuity requirements.

5.1.4. In addition, the solution must strengthen National Treasury's cyber resilience posture through advanced protection against ransomware and other cyber threats. This includes immutable backups, isolated recovery environments (air-gapped capabilities), and alignment with Zero Trust principles to ensure rapid restoration of clean, verified data while minimising operational disruption.

5.1.5. Given National Treasury's dual-site environment comprising a Production site, high availability site and a Disaster Recovery site, the solution must deliver consistent and verifiable data protection, rapid recovery capabilities, long-term retention, and compliance archiving, with data replicated/archived to a secure cloud-based immutable repository to support organisational resilience and regulatory requirements.

5.2. Scope of Work / Business Requirements — Server and Workload Backup

5.2.1. The proposed Cyber Resilience and Data Protection Solution must comply with internationally recognised information security, privacy, business continuity, and cyber resilience standards. At a minimum, the solution must align with ISO/IEC 27001 for Information Security Management Systems (ISMS) and ISO/IEC 27701 for Privacy Information Management. The solution must further demonstrate alignment with ISO/IEC 27031 (or any successor standard), ensuring ICT readiness to support business continuity through the prevention, response, and recovery of ICT-related disruptions.

5.2.2. The solution must also support National Treasury's governance, compliance, and risk management objectives by adhering to all applicable South African legislative and regulatory requirements relating to data protection, privacy, cybersecurity, and public sector financial management. This includes, but is not limited to:

- Protection of Personal Information Act (POPIA): Ensuring the lawful collection, processing, storage, retention, and transmission of personal information.
- Public Finance Management Act (PFMA): Supporting accountability, governance, transparency, auditability, and the effective management of systems underpinning financial management processes.
- Data Sovereignty Requirements: Ensuring that regulated, sensitive, and critical government data is stored, processed, and protected within the borders of South Africa unless otherwise permitted by law or approved by National Treasury.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0: Demonstrating alignment with the framework, including the Govern (GV) function, to

strengthen cybersecurity governance, risk management, resilience, and organisational oversight.

- Other Applicable Regulations and Standards: Complying with any additional national, sector-specific, or government-mandated requirements related to cybersecurity, records management, digital continuity, and information governance.

5.2.3. The successful vendor shall ensure that all solution components, processes, and services—including backup, replication, recovery, retention, archival, immutability, and cyber recovery capabilities—operate in accordance with these standards and regulatory frameworks. The solution must provide the necessary controls, reporting, audit trails, and governance mechanisms to support compliance, reduce regulatory risk, and enhance National Treasury's overall cyber resilience and operational integrity.

5.3. Due Diligence

5.3.1. Environment Discovery and Validation

- Prior to final solution sizing and contract award, the prospective vendor will be afforded the opportunity to perform a comprehensive discovery and validation exercise within the National Treasury environment. The purpose of this exercise is to independently verify the current environment, including but not limited to workload volumes, server and endpoint counts, operating systems, databases, applications, virtual and physical infrastructure components, and any other systems within the scope of this procurement.

- The discovery exercise shall not be limited to existing asset registers or inventory records and must be conducted against the environment as deployed at the time of assessment. The vendor shall validate the accuracy of the collected information against the indicative workload volumes provided in this document and may propose adjustments were justified by the findings.

- A detailed inventory of all operating systems, applications, databases, and supported workloads identified during the discovery process shall be documented and included as an appendix to this document. The validated inventory will be used as the baseline for final solution design, sizing, licensing, implementation planning, and contractual commitment.

5.4. Proposed Backup and Protected Workload Volumes

Scope of Work Component	Quantity
Backup Capacity – Production Environment	480 TB
Backup Capacity – Disaster Recovery Replica	480 TB
Microsoft 365 – Exchange Online Mailboxes	1686
Identity Protection – Microsoft Entra ID Objects (users, groups, and associated configuration)	2490
Professional Services Hours	30 Hours per year (150 Hours)

Note: The workload volumes and professional services effort reflected above are indicative and provided solely for tender response purposes. National Treasury reserves the right to adjust these volumes following the completion of the discovery and validation exercise. Final contracted volumes shall be confirmed and baselined at contract signature. The contract shall include a clearly defined mechanism to accommodate future growth, such as volume uplift bands, scalable licensing models, or agreed rate cards for additional protected workloads and storage capacity.

5.5. Enabling IT Business Continuity

5.5.1. The proposed backup and recovery solution shall form a key component of National Treasury's business continuity and disaster recovery strategy by ensuring the protection, recoverability, and integrity of critical business information.

5.5.2. While backup and restore capabilities will serve as the primary mechanism for recovering lost, corrupted, or inadvertently deleted data, National Treasury acknowledges that certain critical business services may require recovery objectives that exceed the capabilities of traditional backup technologies. In such instances, supplementary continuity mechanisms shall be implemented to achieve the required Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

5.5.3. The solution shall therefore support the following continuity capabilities:

Orchestrated Recovery: To facilitate rapid recovery during large-scale service disruptions or site-wide failures, the solution shall provide automated recovery orchestration capabilities for virtual machine-based applications and their supporting infrastructure. These capabilities must enable the coordinated recovery of multi-tier virtual machine environments — including database, application, and web tiers — in a defined boot-order sequence reflecting application dependencies. Recovery workflows shall automate the provisioning and configuration of compute, storage, and network resources to minimise recovery times and achieve recovery objectives that would be impractical through manual restoration processes.

Cyber Recovery: In the event of a ransomware attack, malware outbreak, or other cyber incident that compromises the integrity of production data, the solution shall support a dedicated cyber recovery capability. This capability shall provide for the isolation of mission-critical backup data within an immutable and logically air-gapped vault, segregated from the primary backup platform and from the customer's production identity domain. The solution shall further provide a network-isolated recovery environment, distinct from the air-gapped vault, into which data can be recovered for testing and validation. Recovery into this isolated environment shall support snapshot-level classification — clean, quarantined, or anomalous — based on integrated malware and ransomware detection, enabling operators to select verified-clean recovery points and confirm that restored data is safe to reinstate into production systems.

5.6. Data Backup Architecture (D2D2C)

5.6.1. The vendor shall provide and manage a Data-to-Disk-to-Disk-to-Cloud (D2D2C) backup architecture that delivers multiple recoverable copies of National Treasury data across separate storage locations and media types.

5.6.2. The solution shall, at a minimum, maintain three recoverable backup copies and shall support recovery operations from each copy independently.

Backup Copy	Frequency and Backup Window	Media Type
Copy 1 – Production Backup Repository located at the designated Production Site	Daily (18:00 – 06:00)	Disk
Copy 2 – Replicated Backup Repository located at the designated Disaster Recovery Site	Daily following successful backup completion (06:01 – 17:59)	Disk

Copy 3 – Immutable Cloud Repository for long-term retention and compliance archiving	Monthly	Cloud

5.6.3. The solution shall ensure data consistency across all backup copies and provide the ability to recover data directly from any of the repositories based on operational requirements and recovery objectives.

5.7. Long-Term Retention and Compliance Archiving (Cloud-Based Immutable Repository)

5.7.1. Long-term retention and compliance archiving services shall be delivered through a managed, air-gapped, immutable cloud-based repository designed to safeguard backup data against accidental deletion, malicious modification, ransomware, and insider threats.

5.7.2. The repository shall provide S3-compatible object storage supporting Write-Once-Read-Many (WORM) immutability capabilities. Backups designated for long-term retention shall be automatically replicated and tiered into this isolated repository in accordance with defined retention policies.

5.7.3. This architecture establishes a logical airgap between operational backups and long-term retention copies while eliminating the operational overhead associated with physical media handling, transportation, and offsite storage services. All archived backup data shall remain encrypted, immutable, and protected from unauthorised deletion throughout the retention period.

5.7.4. The cloud-based immutable repository shall serve as the offsite retention location for National Treasury's two-site architecture (Production and Disaster Recovery), thereby extending the on-premises backup ecosystem without necessitating the establishment of a third physical data centre.

5.8. Backup Policy (Frequency, Retention, Replication and Archiving)

5.8.1. The proposed solution shall fully comply with National Treasury's Data Backup Standard and any future amendments thereto. No deviations from the approved policy shall be permitted without prior written approval from National Treasury.

5.8.2. The solution shall enforce all backup policies through automated policy-based management, leveraging workload discovery, classification, policy inheritance, and automated scheduling to ensure ongoing compliance for all existing and newly provisioned systems.

Backup Type	Retention Period	Media	Storage Location	Replication Frequency
Daily Incremental Backup	14 Days	Disk	Production and Disaster Recovery Sites	Daily after completion of backup window
Weekly Full Backup	4 Weeks	Disk	Production and Disaster Recovery Sites	Weekly upon completion of backup cycle
Monthly Full Backup	12 Months	Cloud	Offsite Immutable Repository	Monthly at month-end
Annual Backup	5 Years	Cloud	Offsite Immutable Repository	Annually, aligned to National Treasury financial year-end

Archive Logs	14 Days	Disk	Production and Disaster Recovery Sites	As determined by application requirements

5.8.3. The policy ensures a layered and resilient backup strategy that supports both operational recovery and long-term archival, while meeting National Treasury's compliance and governance requirements.

5.8.4. "Retention periods in this policy represent the minimum baseline and must be adjusted where National Treasury's records management or statutory requirements mandate longer retention. Where retained backups (including the 5-year Annual Backup) remain within their retention period beyond the expiry or termination of this contract, the vendor must provide for continued read/export access to that retained data, or a complete export of it in an open, portable format, for an agreed transition period following contract expiry, at no additional cost beyond reasonable transition support.

5.9. Periodic Backup Restore Testing

5.9.1. The vendor shall be responsible for leading and coordinating all periodic backup restore testing activities. This includes proactive engagement with both the Infrastructure as a Service (IaaS) provider and National Treasury's Disaster Recovery (DR) teams to validate the integrity, recoverability, and performance of backup data across all tiers.

5.9.2. To ensure consistency and reduce operational overhead, it is strongly recommended that the vendor implement an automated backup validation tool with the following capabilities:

- Verifying the integrity of backup copies without manual intervention.
- Simulating restore scenarios to validate recovery time and data completeness.
- Generating audit-ready reports for compliance and operational assurance.

5.9.3. Automated testing will enhance National Treasury's ability to meet regulatory requirements, reduce recovery risks, and maintain confidence in the backup environment's readiness during real-world incidents.

5.9.4. Automated Recovery Validation: Utilising instant recovery / live mount technology to instantly boot virtual machines and applications directly from the backup repository in an isolated network. This ensures integrity and application consistency without impacting the production environment or storage.

- Blueprint-Based DR Orchestration: Implementing recovery workflows with pre-defined recovery blueprints, including boot-order sequencing, configurable network handling (including IP/MAC preservation or reassignment with post-recovery script execution for DNS and application reconfiguration), required to simulate complex multi-tier application restores, directly validating Recovery Time Objectives (RTOs) through non-disruptive test recovery.
- Continuous Compliance Reporting: Generating automated, audit-ready SLA compliance and recovery reports.
- Proactive Threat Hunting during Testing: Automatically scanning recovery points for known indicators of compromise (IoCs) and malware signatures during the test cycle to ensure that restored data is not only available but also clean and safe for reintroduction. Vendors must specify the depth of scanning available (e.g. hash-based matching vs. full content/pattern-based scanning).

5.10. Data Backup and Storage Infrastructure Technology

5.10.1. National Treasury recommends the deployment of a Zero Trust-aligned data protection platform utilising a linear scale-out architecture that ensures high-performance, immutable data protection, sized to complete backup operations within the designated backup window.

- Hyperconverged, Scale-Out Architecture: The platform shall be built on a converged, scale-out architecture capable of scaling linearly to multi-petabyte environments under a single, unified management plane, without requiring a separate or third-party database engine to manage platform metadata or the backup catalogue.
- Non-Disruptive Lifecycle: Capacity and performance scaling, as well as software lifecycle upgrades, must not require a forklift hardware replacement or a rebuild of the existing protection environment.
- No Single Point of Failure: The platform shall provide high availability across all of its own components such that the failure of any single node or component does not result in downtime of the backup or recovery service.

5.10.2. These recommendations are based on industry-standard deployment patterns. Vendors are encouraged to propose alternative or enhanced solutions that meet the requirements outlined in this section and offer improved cost-efficiency, scalability, and performance.

5.10.3. Unstructured Data Management

- Direct-to-Target Data Ingestion: The solution must support direct, incremental-forever ingestion of unstructured data to cloud or on-premises object storage without requiring intermediary staging areas or primary storage landing zones.
- Native Data Optimisation & Security: The solution must provide built-in indexing, compression, and encryption for all unstructured data sets.
- Federated Search and Granular Recovery: The solution must enable global federated search and granular recovery of files and folders across all backup locations.

5.11. Databases

5.11.1. The solution must provide deep, application-aware protection for National Treasury's enterprise databases, including, at a minimum:

- Automatic Discovery and Protection: New database instances and individual databases must be automatically discovered and brought under policy-based protection without requiring per-database manual configuration.
- Granular Recovery: Recovery must be supported at the database or instance level across all protected database engines, with finer-grained recovery — including tablespace or pluggable-database (PDB) level for Oracle and collection level for MongoDB — supported where the database engine's architecture allows, in addition to full instance recovery.
- Parallel Capture of Data and Log Files: The solution must support parallel, application-consistent capture of database data files and transaction/archive log files, enabling point-in-time recovery between full or incremental backups.
- Support for Encrypted Databases: The solution must be able to protect databases that have native, engine-level encryption enabled, without requiring encryption to be disabled for backup to succeed.
- Mountable Copies for Test/Dev: Backup copies of databases must be mountable directly to an alternate host for test, development, or rapid access use cases, without requiring a full restore.

- Native Database Tool Integration: Where applicable to the database engine, the solution must integrate with native database backup utilities (e.g. RMAN for Oracle) rather than relying solely on generic file-level or storage-level snapshots.

5.11.2. Vendors must specify which database engines in use at National Treasury are supported, and the recovery granularity available for each.

5.12. Global Indexing and Storage Optimisation

5.12.1. Automatic Optimisation: Compression and deduplication must be performed automatically and optimised per workload type, without requiring manual tuning or separate background administrative processes.

5.12.2. Global File-Level Indexing: The solution must perform file-level indexing globally across protected workloads, enabling search-driven recovery of individual files without needing to know in advance which backup or snapshot contains them.

5.13. Security, Encryption, and Cyber Resiliency

5.13.1. The solution must incorporate advanced data protection mechanisms to ensure the confidentiality, integrity, and availability of backup data. At a high level, key features must include:

- Encryption: End-to-end encryption of data both in transit (TLS 1.2+), at rest (AES-256), and between platform nodes, enabled by default and not configurable as an optional setting. Encryption must not require additional hardware or measurably degrade backup or restore performance.

- Deduplication: Efficient data deduplication to reduce storage footprint and enhance performance.

- Replication and Archiving: Secure replication across the Production and DR sites, and archiving to an immutable, object-storage-based cloud repository, to ensure redundancy and resilience. Replication should be pull-based (initiated by the receiving site) so that no inbound ports need to be opened on the receiving cluster to support ongoing replication.

- Identity Resilience: The solution must provide a unified Identity Resilience framework for hybrid Microsoft environments (Active Directory and Entra ID), covering National Treasury's full Entra ID estate of approximately 2,490 identity objects, strictly adhering to a Zero Trust Security architecture. The platform shall ensure that identity data is architecturally isolated and inherently unchangeable. Detailed identity protection and recovery requirements are set out in Section 3.2.

- Ransomware Protection: The solution must include capabilities to detect, prevent, and recover from ransomware attacks, ensuring backup data remains uncompromised and recoverable.

- Continuous or Near-Continuous Data Protection: For workloads requiring more aggressive recovery points than periodic snapshots can deliver, the solution **should support short-interval backup or equivalent continuous protection mechanisms**, enabling recovery to a specific point in time within a configurable protection window.

- Retention Lock and Legal Hold: The solution must support retention-lock-enforced immutability through a simple, auditable mechanism, such that backups cannot be overwritten, prematurely expired, or altered before their retention period expires, with no administrative override to disable immutability. Changes to retention locks and holds, and other destructive or sensitive operations, must themselves be governed by a quorum (multi-approver) authorisation process to protect against a single compromised credential. This multi-approver capability must be a native, built-in feature of the platform, not a separately licensed module or a workflow requiring separate download or integration. The solution must also support placing backups on legal hold and tracking and monitoring legal hold status via a dashboard.

5.14. Ransomware Response Team

- The vendor must provide National Treasury with access to a dedicated Ransomware Response Team (RRT) to support the organisation in the event of a suspected or confirmed ransomware or other cyber-extortion incident affecting in-scope systems. The Ransomware Response Team must operate as an extension of National Treasury's existing Cyber Event Response Team and the broader incident response process, and must, at a minimum, provide:

- 24x7x365 Availability: A dedicated incident hotline and escalation path, always staffed and available, with a guaranteed initial response within a defined time window (e.g. within 1 hour of a Severity 1 incident being logged).

- Specialist Skills: Access to backup and recovery specialists, ransomware forensics analysts, and recovery architects with demonstrable experience responding to live ransomware events in comparable public-sector or regulated environments.

- Recovery Point Triage: Rapid identification of the last known-clean recovery point(s) across affected workloads, using automated anomaly detection and indicator-of-compromise (IoC) scanning of backup data, informed by the sensitive data discovery and classification capability described in Section 4 to support business-impact assessment alongside technical recovery.

- Clean-Room Recovery Support: Hands-on support to stand up an isolated recovery (clean-room) environment, validate recovered data is free of malware or backdoors, and assist with the phased reintroduction of recovered systems to production.

- Coordination with National Treasury Stakeholders: A named incident lead and communication cadence to keep National Treasury's IT, security, and executive stakeholders informed throughout the incident lifecycle, including post-incident root cause and lessons-learned reporting.

- Runbook and Readiness Testing: Development of a joint ransomware recovery runbook with National Treasury, with at least an annual joint tabletop exercise or live recovery test to validate response readiness ahead of any actual event.

5.14.1. The structure, escalation matrix, and named resources of the proposed Ransomware Response Team must be documented as part of the vendor's response to this Scope of Work.

5.15. Ransomware Recovery Warranty

5.15.1. Vendors must offer a Ransomware Recovery Warranty covering all in-scope, correctly configured and protected workloads, committing to the recoverability of data backed up in accordance with the agreed Backup Policy (Section 2.6). At a minimum, the warranty must address:

- Recoverability Guarantee: A written commitment that data protected in line with the agreed backup policy will be recoverable in the event of a ransomware attack, subject to the workload having been correctly configured and actively backed up at the time of the event.

- Defined Remedy: Where the vendor's platform fails to deliver a recoverable copy of in-scope data due to a defect or failure of the Solution itself, the vendor must specify the financial or service-credit remedy available to National Treasury, and the process for invoking it.

- Exclusions: Any exclusions to the warranty (e.g. workloads excluded from scope, unconfigured or unmonitored systems, failure to act on prior alerts) must be explicitly stated and agreed with National Treasury, rather than implied.

- Claims Process: A clear, time-bound process for National Treasury to notify the vendor of a suspected warranty event, and for the vendor to validate the claim and respond.

5.15.2. The full terms of the proposed warranty, including coverage limits, qualifying conditions, and claims process, must be submitted as part of the vendor's response and will be evaluated as part of this Scope of Work.

5.16. Data Integrity and Chain of Custody

5.16.1. The solution must provide verifiable assurance that backup data has not been altered, corrupted, or tampered with at any point in its lifecycle. At a minimum, the solution must:

- Cryptographic Fingerprinting: Create and maintain a cryptographic fingerprint (e.g. checksum or hash) of backup data at the time of capture.
- Lifecycle-Wide Verification: Verify data integrity across the entire data lifecycle, including local retention, replication to the DR site, and archival to the cloud-based immutable repository, with continuous background validation rather than verification only at the point of backup or restore.
- Chain-of-Custody Evidence: Support chain-of-custody evidence suitable for compliance and audit purposes, demonstrating that a given recovery point is identical to what was originally captured.

5.17. Access Control and Security Governance

- Multi-Factor Authentication: The platform shall support multi-factor authentication, including TOTP-based authenticator apps, for all administrative and user access.
- Object-Level RBAC: Role-based access control must be configurable at the object level (e.g. specific VMs, databases, or file sets), not only at the cluster or global level.
- Multi-Tenancy and Enterprise Identity Integration: Where multi-tenant access is required, the solution must integrate with National Treasury's enterprise identity provider(s) for authentication and access scoping.
- Supply-Chain Risk Reduction: The platform must not allow third-party plug-ins or marketplace applications that would introduce additional supply-chain risk into the protection environment.

5.18. Threat Hunting and Containment

5.18.1. In addition to the Ransomware Response Team described in Section 2.9.1, the underlying platform must provide the following standing threat hunting and containment capabilities:

- Offline Hunting on Backup Data: Threat hunting must be performed natively against backup data itself, without requiring a separate third-party security tool for scanning. Hash-based threat hunting shall complete without mounting snapshot data; deeper rule- or pattern-based scanning (e.g., YARA-based) may mount snapshot data for content inspection, but only within the vendor's own backup infrastructure, never requiring export to or ingestion by external tooling.
- Rapid, Pre-Computed Scanning: In addition to deeper content-based scanning, the solution must support rapid hash-based matching against a pre-computed catalogue of known indicators of compromise, enabling large numbers of backup snapshots to be screened in seconds without mounting each one individually.
- Cross-Workload Investigation: Investigation must be supported across physical, virtual, and NAS/unstructured workloads from a single workflow.
- Quarantine: Snapshots or backups identified as infected must be quarantined within the platform, isolating them from standard recovery workflows without requiring deletion, and preventing them from being inadvertently restored into production.
- Surgical Recovery of Infected Areas: Where only specific files or objects within a backup are found to be compromised, the solution must support recovering only the affected areas, rather than requiring a full server or volume rollback.

- Validated Clean Recovery Point Before Restoration: Before any data is moved into a recovery environment, the solution must identify and validate a clean recovery point using its integrated threat intelligence and scan results, rather than relying on a trial-and-error restore approach.

- Self-Updating Threat Intelligence: Threat intelligence feeds used for detection must update automatically, without manual intervention or reliance on a third-party agent.

- These threat hunting and containment capabilities must be delivered natively by the proposed platform and must not rely on third-party malware-scanning agents or separate appliances in the data path.

5.19. Management, Monitoring, and Reporting

5.19.1. The solution must offer comprehensive monitoring and reporting capabilities to support proactive management and operational transparency. Requirements include:

- Native Monitoring Tools: Full utilisation of built-in monitoring features for real-time visibility into backup job status, performance metrics, and system health.

- Integration with ITSM/ITOM Platforms: The solution must support integration with National Treasury's existing IT Service and Operations Management tools to enable centralised oversight and incident response, including role-based, SSO-group-tied self-service recovery requests initiated from the ITSM platform.

- Infrastructure as Code: The platform should support integration with infrastructure-as-code tooling such as Ansible and Terraform for automation of platform configuration tasks.

- Coverage Reporting: The backup system must provide coverage analysis reports to identify unprotected assets and coverage gaps.

- API-First Architecture: The platform shall expose fully documented, supported APIs covering all platform operations, in support of integration with National Treasury's ITOM and SIEM tools. Graph or other modern API paradigms will be considered an advantage. Vendors are encouraged to describe any platform-provided environment for testing API calls and scripting against the platform.

- A single management plane to capture all events, feed them to SIEM tools via webhooks, and produce compliance and audit reports.

- A single operations plane to manage all data protection, disaster recovery, and cyber resilience capabilities (anomaly detection, threat monitoring, threat hunting, sensitive data discovery, orchestrated recovery, and identity access management) across the on-premises data centre and Microsoft 365 environment.

5.20. Automation and Backup Failure Prevention

5.20.1. The solution must incorporate intelligent automation capabilities to proactively detect and mitigate potential backup failures. This includes:

- Predictive Analytics: The system should analyse historical trends and system behaviour to anticipate failures before they occur, using AI-driven storage, frequency, and bottleneck prediction.

- Automated Alerts and Remediation: Upon identifying anomalies or risks, the solution must automatically notify the responsible backup engineer and, where possible, initiate predefined remediation workflows.

- Integration with RDBMS and Application Layers: The backup platform should integrate with relational database management systems and other critical application layers to monitor backup health and ensure data consistency.

5.21. Scalability

5.21.1. The infrastructure underpinning the solution must be designed with elastic scalability to accommodate unforeseen data growth and evolving business requirements without disrupting ongoing operations. Key expectations include:

- Modular Architecture: The solution should support scaling of storage, compute, and network resources.
- Capacity Planning: Vendors are expected to implement cost-effective capacity management strategies while ensuring that performance and retention policies are not compromised.
- Non-Disruptive Expansion: Scaling operations — whether on-premises or in the cloud — must be seamless and not require downtime or reconfiguration of existing backup jobs.
- Data Intelligence & Auto-Balancing: Automated capacity management that intelligently redistributes data across the system.

5.21.2. This ensures that National Treasury's backup environment remains resilient, responsive, and future-ready.

5.22. Scope of Work / Business Requirements — Microsoft 365 and Identity Protection

5.22.1. National Treasury's Microsoft 365 and identity estate is in scope for this engagement, covering Exchange Online and the Entra ID identity layer, with protection extending to the broader M365 workload set as adopted.

5.23. Microsoft 365 – Exchange Online

The solution must provide comprehensive backup and recovery of Exchange Online mailboxes across National Treasury's approximately 1,686 licensed users, with granular recovery of individual items (emails, calendar items, contacts) as well as full mailbox restore capability. Backups must be retained independently of Microsoft's native retention policies, ensuring recoverability beyond the limitations of the Recycle Bin and
native compliance holds.

5.24. Identity Protection – Entra ID

5.24.1. The solution must provide backup and recovery coverage for National Treasury's Entra ID tenant, covering approximately 2,490 identity objects (users, groups, and associated configuration). This includes:

- Surgical recovery of individual Entra ID objects (users, groups, application registrations) without requiring a full tenant restore, including the ability to compare current identity attributes (e.g. user, group, or role attributes) against a prior backed-up state to identify and roll back malicious or accidental changes at the attribute level.
- Full Active Directory forest recovery via a unified, orchestrated workflow, in addition to the surgical object-level recovery described above, and the ability to recover Entra ID objects and configuration to an isolated state or alternate tenant where required for forensic or recovery purposes.
- Detection of risky changes and privilege escalation within the identity environment, with alerting aligned to a Zero Trust architecture. Vendors must specify alert latency and the scope of coverage across both the Active Directory and Entra ID layers of the hybrid identity environment, including any differences in detection capability or alerting maturity between the two.
- Native integration with Microsoft Entra ID, ingesting threat alerts directly and correlating all activity performed by a compromised identity across both Active Directory and Entra ID. The solution must support both cherry-picked reversal of specific malicious changes and bulk-revert of all attacker actions, while preserving legitimate changes made by the same identity.
- Recovery workflows that support re-establishing hybrid identity synchronization (Active Directory to Entra ID) as part of recovery, where applicable. Vendors must clearly state the

current level of automation for this specific step (e.g., fully orchestrated vs. partially manual) as distinct from AD forest recovery and Entra ID tenant recovery individually, and must provide an indicative recovery timeline for a complete hybrid identity restoration, including directory sync realignment.

5.24.2. Identity protection capabilities must be positioned to support National Treasury's broader cyber resilience posture, given that identity compromise is a leading vector for ransomware and data-destruction attacks against public-sector entities.

5.25. Sensitive Data Discovery and Compliance

5.25.1. The solution must include native sensitive data discovery and classification capability, enabling National Treasury to understand its exposure to data-protection and privacy risk before, during, and after a cyber event. At a minimum, the solution must:

- Cover all in-scope unstructured data, Microsoft 365 content, and structured data held in SQL databases.
- Require no additional software or hardware beyond the core backup and recovery platform to perform discovery and classification.
- Identify sensitive data (e.g. personal information regulated under POPIA, financial records) in protected (backed-up) locations at a minimum. Where the solution can also identify sensitive data in locations not yet under backup protection, vendors must describe the mechanism and scope — for example, whether this applies only to cloud-native storage discovered independently of backup status, or extends to on-premises systems, which may require the system to first be onboarded to a backup policy before it can be scanned.
- Surface classification results in a manner that supports rapid business-impact assessment during a ransomware or data-breach event, including which sensitive data categories were present in affected systems.

5.25.2. This capability must integrate with the anomaly detection and threat hunting capabilities described in Section 2.9, and specifically with the Recovery Point Triage step performed by the Ransomware Response Team (Section 2.9.1), so that the sensitivity of data affected by a security event is visible as part of incident triage, not as a separate manual exercise.

5.26. Service Level Agreement Requirements

5.26.1. Front-End Server (Physical and Virtual)

- National Treasury defines three service tiers based on the business criticality of the environment. The following SLA metrics apply across tiers, with performance targets measured and reported as specified
- These SLA metrics are critical to ensuring data availability, operational resilience, and compliance with National Treasury's business continuity and disaster recovery objectives.

Table 1

Tier	Description	Example Workloads	Target RPO	Target RTO
1	Mission-critical	Core financial systems, identity	≤ 1 hour	≤ 4 hours
2	Important but non-mission-critical	Line-of-business apps	≤ 4 hours	≤ 24 hours
3	Standard / non-critical	Low-impact systems / test environments	≤ 24 hours	≤ 72 hours

Table 2

Measurement	Frequency	Target
Backup Success	Daily	≥ 95% of scheduled backup jobs must complete successfully
Replication Success	Daily	100% of successfully completed backups must be replicated to the designated DR site
Restore	As requested, or DR testing	100% of the 95% successfully backed-up systems must be restorable; any system that fails its scheduled backup must be remediated and successfully backed up within the next scheduled backup window, so that no system remains permanently outside the restore commitment
Backup Testing	Quarterly (every 3–4 months)	100% of tested backups must pass restore validation

5.27. Scope Inclusions

5.27.1. This Scope of Work encompasses all components necessary to ensure the secure, reliable, and compliant backup of National Treasury's data assets, regardless of hosting environment (on-premises, Production/DR, or cloud) or platform (servers or SaaS applications). The scope includes, but is not limited to:

- Backup and recovery software licenses.
- Backup infrastructure (e.g. master and media servers, storage units, cloud-based immutable repository storage).
- Network connectivity and bandwidth provisioning for replication and restore.
- Encryption and security mechanisms.
- Monitoring, reporting, and alerting tools.
- Integration with ITSM and RDBMS platforms.
- Automation and orchestration tools for backup validation and failure prevention.
- Professional services for implementation, configuration, and training.
- Ongoing support and maintenance of all infrastructure deployed towards the delivery of this solution.
- Capacity management and reporting.

5.28. Training and Transfer of Skills

5.28.1. For a successful implementation and adoption of the Cyber Resilience and Data Protection Solution at National Treasury, training will be essential across multiple user groups, aligned with National Treasury's operational structure and technical environment.

Table 3

Training Category	Target Audience	Objectives
Backup Administrators / Infrastructure Teams	Backup engineers, system administrators	Manage, monitor, and maintain the Solution, including policy configuration, monitoring dashboards, restore testing, and integration with ITSM tooling
Disaster Recovery & Business Continuity Teams	DR coordinators, continuity planners	Validate backup readiness, plan and execute DR tests, and track SLA compliance in coordination with the infrastructure and platform teams
Security & Compliance Teams	Information security officers, compliance managers	Ensure data protection aligns with POPIA, the PFMA, NIST CSF 2.0, and National Treasury policy; oversee audit logging and data sovereignty compliance

5.29. Professional Services for the Solution

5.29.1. Below is a list of professional services typically associated with a Cyber Resilience and Data Protection Solution engagement, tailored for National Treasury's environment:

5.29.2. Assessment & Planning

- Backup environment assessment (current-state analysis).
- Data classification and workload prioritisation.
- RTO/RPO alignment and gap analysis.
- Network and storage capacity planning.
- Compliance and regulatory readiness review (e.g. POPIA, PFMA, NIST CSF 2.0, ISO/IEC 27031).

5.29.3. Solution Design

- Architecture design for on-premises backup across Production and DR sites, with cloud-based long-term retention.
- Backup policy and retention strategy development.
- Integration planning (e.g. with ITSM/ITOM, RDBMS).
- Security and encryption framework design.
- High availability and disaster recovery planning.

5.29.4. Implementation & Configuration

- Deployment of backup infrastructure (disk and cloud-based immutable repository).
- Configuration of backup schedules, policies, and replication.
- Setup of monitoring, alerting, and reporting tools.
- Integration with identity and access management (IAM), including Entra ID.
- Network optimisation for backup traffic.

5.29.5. Data Migration & Seeding

- Initial data seeding to backup repositories.
- Migration of legacy backup data, where applicable.
- Validation of data integrity post-migration.

5.29.6. Testing & Validation

- Backup and restore testing (including DR scenarios).
- Performance benchmarking.
- SLA validation and reporting setup.
- Security and access control testing.

5.29.7. Training & Knowledge Transfer

- IT support and backup administrator training.
- DR team and compliance team enablement.
- Documentation handover, including backup architecture and data flow documentation.

5.29.8. Ongoing Support & Optimisation

- Managed services for backup operations.
- Periodic health checks and performance tuning.
- SLA monitoring and reporting.
- Policy reviews and updates.
- Incident response and forensic recovery support, delivered via the Ransomware Response Team described in Section 2.9.1.
- Isolation and containment of cyber threats.
- Forensic investigation and root cause analysis of cyber events.
- Recovery and remediation of cyber events.
- Detailed requirements in Appendix A: Section 16.

5.29.9. Compliance & Audit Support

- Audit trail configuration and reporting.
- Retention policy enforcement.
- Support for regulatory audits and internal reviews.

5.29.10. Professional Services Roles for the Solution

5.29.11. Key roles typically involved in delivering Professional Services for the solution, tailored for National Treasury's environment:

- Backup Solutions Architect: Designs the overall solution architecture (on-premises, with cloud-based long-term retention); aligns the solution with National Treasury's business continuity, compliance, and scalability needs; defines backup policies, retention strategies, and integration points.

- Backup Implementation Engineer: Installs and configures backup software and infrastructure; sets up replication, encryption, and monitoring tools.

- Data Migration Specialist: Manages initial data seeding and migration from legacy systems; ensures data integrity and consistency during transition; coordinates with storage and network teams for performance optimisation.

- Disaster Recovery Consultant: Develops and tests DR scenarios using backup data; validates RTO/RPO targets and restore capabilities; coordinates with National Treasury's DR and IaaS teams.

- Security & Compliance Analyst: Ensures backup processes align with POPIA, the PFMA, NIST CSF 2.0, ISO/IEC 27031, and National Treasury policy; configures encryption, access controls, and audit logging; supports internal and external audits.

- Monitoring & Reporting Specialist: Implements dashboards and reporting tools; tracks SLA metrics (e.g. backup success, restore rates); integrates with ITOM platforms. The SLA will include but is not limited,

- Service Levels (24x7x365)
- Penalty fees for SLA non-compliance, as defined in Section 5.26 (Service Level Agreement Requirements)
- Confidentiality
- Third Party work etc.

- Project Manager: Oversees the implementation lifecycle of the solution; manages timelines, resources, and stakeholder communication; ensures deliverables meet National Treasury's expectations.

- Support & Optimisation Engineer: Provides ongoing technical support and issue resolution; conducts periodic health checks and performance tuning; recommends improvements and updates.

SECTION B: CONDITIONS OF BID

6. PART 1: EVALUATION CRITERIA

6.1. The details of the evaluation phases are outlined below:

Table 4: Evaluation Criteria

Phase 1	Phase 2	Phase 3	Phase 4
Mandatory requirements	**Legislation and other standard bidding Requirements**	**Functionality Requirements**	**Price and Specific Goals**
Compliance with mandatory requirements	Compliance with legislative and other bid requirements	Minimum threshold of 70%	Bids evaluated in terms of the 80/20 preference system

6.2. Phase 1: Mandatory Requirements

6.2.1. Pricing Schedule

6.2.1.1. Bidders are required to submit responsive bids by completing all pricing on the provided pricing schedule (Annexure C SBD 3.3). Non-submission of the pricing schedule (Annexure C) will invalidate the bid.

6.2.1.2. The pricing schedule (Annexure C) provided in this bid forms an integral part of the bid document, and bidders must ensure that it is completed without changing the structure thereof.

6.2.1.3. Bid prices must be inclusive of all costs, and VAT.

6.3. Mandatory Functional Requirements (Please complete Annexure E at the end of the documents)

6.3.1.1. This phase will be evaluated on a Pass/Fail basis. Bidders must comply with all mandatory requirements to qualify for further evaluation.

6.3.1.2. A bidder must meet all mandatory requirements before their proposal can move to the next stage of the evaluation process.

6.3.1.3. The mandatory requirements are the minimum standards that National Treasury requires and are not negotiable. They are assessed before the technical, implementation, functionality, and pricing evaluations.

6.3.1.4. Only bidders who pass all mandatory requirements will be considered for the scored evaluation phases.

6.3.1.5. Bidders must tick "Yes" or "No" against every item and attach the supporting evidence specified. A single "No", an unanswered item, or unsubstantiated evidence against any mandatory requirement below will render the bid NON-RESPONSIVE and will not proceed to scored evaluation, regardless of price or technical score elsewhere in the submission.

6.4. Phase 2: Legislative and other standard bidding documents

6.4.1. Legislative requirements

6.4.2. It is also a requirement for bidders to submit the other legislative documents as detailed below.

6.4.3. SBD 1 invitation form to bid.

6.4.4. SBD 4 bidder's disclosure.

6.4.5. SBD 6.1 preference points claim form.

6.4.6. Central Supplier Database – A Central Supplier Database report must be submitted

6.4.7. Bidders are required to submit proof of educational qualification(s) for all resources required.

6.4.8. All foreign qualifications must be accompanied by a South African Qualifications Authority (SAQA) certificate of evaluation.

6.4.9. In case of Joint Venture, Consortium, Trust, or Partnership, a signed teaming agreement is required with the partner.

6.4.10. CIPC documents

6.4.11. Shareholding portfolio by proof of registration of the company with Companies Intellectual Property Commission. An additional document detailing the shareholding of the bidder in an organogram format in support of the proof of company registration must be submitted by bidders at the closing date and time.

6.4.12. Failure to submit the documents indicated above even after the bidder has been notified and given a maximum of seven calendar days to rectify may invalidate the bid.

6.5. Phase 3: Functionality Evaluation

6.5.1. During this phase, bidders' responses will be assessed based on functionality. To proceed to the next evaluation phase, bidders must achieve a minimum technical functionality score of **70%**. Only bidders who meet this threshold in Phase 3 will be invited to deliver an online presentation. Bidders who fail to achieve the minimum threshold will be disqualified from further evaluation.

6.5.2. To proceed to the pricing and specific goals evaluation, bidders must meet the minimum threshold of 70% on the online presentation to qualify for further evaluation.

6.5.3. Bidders are required to submit supporting documentation for all functional requirements as part of their bid submission. The Bid Evaluation Committee (BEC) will assess and score each bid based solely on the submitted documentation and the information provided. Failure to provide adequate supporting documents may result in a lower functionality score.

6.5.4. Each criterion will be assigned a score, which will then be multiplied by the designated weighting for that criterion. The total score will be calculated by summing these weighted scores and expressing the result as a percentage of the highest possible score. Bidders are encouraged to ensure that their submissions are complete and clearly demonstrate compliance with the functional requirements.

Table 5: Functional Evaluation

No.	Technical Evaluation Criterion	Weight	Rating Scores
1	**Company Experience**	**15**	Ratings
1.1	**Proven Track Record** Three (3) contactable reference letters	**15**	**1 - Poor** 1 contactable reference letter

	within the past ten (10) years from the Public Sector or a large enterprise for the successful implementation and support of an enterprise backup and recovery solution. The reference letters should be: • On the client's letterhead • Indicate the description of the backup services rendered • Indicate the actual dates of the contract - start and end date • Be dated and signed • Confirm completed and satisfactory status **Qualifier**: The letter should state all the points above, letter not relevant; failure to comply with the above, the letter will be allocated the lowest score. Incomplete or ongoing projects will not be considered. Where an extension has been granted, the bidder must have completed the term of the initial contract.		**2 - Fair** 2 contactable reference letters **3 - Satisfactory** 3 contactable reference letters **4 - Good** 4 contactable reference letters **5 - Excellent** 5 contactable reference letters
KEY PROJECT EXPERTISE, QUALIFICATION, AND EXPERIENCE — 45			
2.1	**Key resource qualifications and experience**		
2.1.1	**Project Manager X1: Qualifications** Bachelor's Degree in Information Technology, Computer Science, Information Systems, Software Engineering, Computer Engineering, Project Management, Business Management, or any other relevant ICT qualification. Please attach: **Matric Certificate and all relevant qualification as stated above.**	**10**	**5** = Matric certificate and Honours Degree or Post Graduate Diploma (NQF 8) or higher, with PMP / PRINCE2 or equivalent certification **4** = Matric certificate and Bachelor's Degree / Advanced Diploma (NQF 7) **3** = Matric certificate and National Diploma (NQF 6) **2** = Matric certificate and Higher Certificate (NQF 5) **1** = Matric (NQF 4) or less
2.1.2	**Project Manager: Experience** Minimum of five (5) years' experience in managing enterprise backup, disaster recovery, infrastructure or cyber resilience implementation projects.	**15**	**5 =** 8 years or more relevant experience **4 =** 6 - 7 years relevant experience **3 =** 5 years' relevant experience **2 =** 3 - 4 years relevant experience **1 =** 2 years or less relevant experience
2.1.3	**Backup Solution Engineer X1: Qualifications** National Diploma in Information Technology / Computer Science / Electrical Engineering/Technician or relevant field, and a valid OEM technical	**10**	**5 =** Matric certificate and Honours Degree or Post Graduate Diploma (NQF 8) or higher, with relevant advanced OEM certification **4 =** Matric certificate and Bachelor's Degree / Advanced Diploma (NQF 7), with relevant OEM professional certification

	certification for the proposed backup solution. **Please attach: Matric Certificate and all relevant qualification as stated above.**		**3 =** Matric certificate and National Diploma (NQF 6), with relevant OEM certification **2 =** Matric certificate and Higher Certificate (NQF 5), with OEM foundation certification **1 =** Matric or less, with no relevant OEM certification
2.1.4	**Backup Solution Engineer: Experience** Minimum of five (5) years' experience in the implementation, configuration, migration and support of enterprise backup and recovery solutions.	**10**	**5 =** 8 years or more relevant experience **4 =** 6 - 7 years relevant experience **3 =** 5 years relevant experience **2 =** 3 - 4 years relevant experience **1 =** 2 years or less relevant experience
3	**Methodology and Approach** **Qualifier: Methodology that is clear, relevant, feasible, and supported by evidence.** **Bidders to submit a Methodology for the backup and cyber resilience solution covering, amongst others:**	**40**	**Rating Scores**
3.1	**Describe the proposed backup and recovery architecture and provide evidence.** Detailed narrative outlining the end-to-end backup and recovery solution, including: • Protection of physical, virtual, database, application and cloud workloads • Backup appliances at the primary data centre and high availability location • Replication between locations • Cloud archive facility • Immutable backup capability • Ransomware detection and recovery • Deduplication and compression • Encryption at rest and in transit • Scalability and capacity management • Integration with the National Treasury infrastructure • Recovery Point Objective and Recovery Time Objective management • Monitoring, alerting and reporting **Qualifier:** Evidence of architecture diagrams, OEM datasheets, screenshots and sample reports.	**15**	**5= Excellent** 12 Requirements Comprehensive architecture description covering all requirements, with clear supporting evidence including architecture diagrams, OEM datasheets, screenshots, and sample reports. Solution demonstrates full functionality, integration, security, resilience, and recovery capabilities. **4 = Good** 10 to 11 Requirements Detailed architecture description covering most requirements with adequate supporting evidence including architecture diagrams, OEM datasheets, screenshots, and sample reports. Demonstrates strong backup, recovery, security, monitoring, and integration capabilities with only minor gaps. **3 = Satisfactory** 7 to 9 Requirements Adequate architecture description covering most requirements. Supporting evidence is provided including architecture diagrams, OEM datasheets, screenshots, and sample reports but may lack detail in some areas. Solution

			meets minimum functional requirements. **2 = Fair** 4 to 6 Requirements Partial architecture description covering some requirements. Supporting evidence including architecture diagrams, OEM datasheets, screenshots, and sample reports is limited, incomplete, or lacks sufficient detail to demonstrate full capability. **1 = Poor** 1 to 3 Requirements Limited architecture description addressing few requirements. Minimal or no supporting evidence including architecture diagrams, OEM datasheets, screenshots, and sample reports provided. Solution capability and compliance cannot be adequately demonstrated.
3.2	**Implementation, Migration and Support** Description of the implementation and migration approach, support structure and service management arrangements: • Project implementation methodology • Detailed project plan with activities, dependencies and milestones • Discovery and assessment of the existing environment • Solution design and configuration • Backup data migration or transition approach • Testing and acceptance process • Cutover and rollback plan • Risk and issue management • OEM accreditation and authorization • Local support structure • Escalation process flows with contact roles • Service Level Commitments, response and resolution times **Qualifier:** Evidence of the project plan, implementation methodology, OEM accreditation, support model, escalation matrix.	**15**	**5 – Excellent=** 11 – 12 relevant evidence with comprehensive and well-documented approach covering all requirements. Detailed project plan, migration strategy, OEM accreditation, support model and escalation process evidence provided. Minimal implementation risk. **4 – Good=** 8 – 10 relevant evidence that addresses most requirements with adequate detail and supporting evidence. Project approach, migration, support and commitments are clearly defined. Low implementation risk. **3 – Satisfactory=** 6 – 7 relevant evidence that meets minimum requirements. Implementation, migration, and support approach are provided but limited details in some areas. Moderate implementation risk. **2 – Fair=** 4 – 5 relevant evidence that partially addresses requirements. Key information or supporting evidence is incomplete or unclear. High implementation risk. **1 – Poor=** 0 – 3 relevant evidence that fails to adequately address requirements. Significant gaps in methodology, migration or support evidence provided. Very high implementation risk.

3.3	**Training, Skills Transfer and Knowledge Transfer** Describe the proposed training and knowledge transfer approach, including: • Formal OEM administrator training • Operational handover • Skills transfer during implementation • Knowledge transfer workshops • As-built documentation • Standard operating procedures • Backup and recovery runbooks • Disaster and cyber recovery exercises **Qualifier:** Evidence of training plan, informal course outlines to NT technicians, knowledge transfer plan, training manual documentation and certification arrangements.	10	**5 – Excellent** = 8 and more relevant evidence of comprehensive training and knowledge transfer approach covering all requirements. Formal OEM training, skills transfer, workshops, training manual documentation, runbooks, recovery exercises, and certification arrangements are clearly defined. **4 – Good=** 6 – 7 relevant evidence of training and knowledge transfer approach addresses most requirements with adequate detail and supporting evidence. Training, training manual documentation, and handover activities are well defined. **3 – Satisfactory=** 4 – 5 relevant evidence that meets minimum requirements. Training, skills transfer, and training manual documentation are provided but with limited detail or supporting evidence in some areas. **2 – Fair=** 2 – 3 relevant evidence that partially addresses requirements. Training, knowledge transfer, or training manual documentation plans are incomplete, unclear, or insufficiently evidenced. **1 – Poor=** 0 – 1 relevant evidence that fails to adequately address training and knowledge transfer requirements. Limited or no evidence of training, training manual documentation, handover, or certification arrangements.
	Total	**100**	
	THRESHOLD	**70%**	

TABLE 2: ON-LINE PRESENTATION EVALUATION

BACKUP SOLUTION – ONLINE PRESENTATION EVALUATION				
No.	**Evaluation Criterion**	**Weight**	**Demonstration / Evaluation Requirements**	**Rating Scores**
1	**BACKUP SOLUTION CAPABILITIES (ONLINE)**	**30**		
1.1	**Solution Architecture, Onboarding and Deployment**	**15**	• Planning and deployment of the backup solution • Configuration of backup infrastructure • Integration with existing infrastructure	0 = 1 – Poor 1 = 2 – Fair 2 = 3 – Satisfactory 3 = 4 – Good 4 = 5 – Excellent

			• Training of administrators/users • System support and maintenance	
1.2	**Demonstrate Backup and Recovery Process**	**15**	• Backup of physical and virtual servers • Backup scheduling and policies • Full and incremental backup capabilities • File/folder recovery • Full VM/server recovery • Microsoft 365 backup and recovery • Automated backup verification • Retention and recovery-point configuration	0–1 = 1 – Poor 2 = 2 – Fair 3 = 3 – Satisfactory 4–5 = 4 – Good 6+ = 5 – Excellent
2	**DISASTER RECOVERY CAPABILITIES**	**15**		
2.1	**Demonstrate Disaster Recovery and Business Continuity Capabilities**	**15**	• Recovery Point Objective (RPO) • Recovery Time Objective (RTO) • Replication to DR environment • Automated failover/failback • Recovery of critical applications • DR testing without impacting production • Demonstration of recovery from a simulated disaster	0–1 = 1 – Poor 2–3 = 2 – Fair 4–5 = 3 – Satisfactory 6–7 = 4 – Good 8+ = 5 – Excellent
3	**SECURITY FEATURES**	**10**		
3.1	**Demonstrate Backup Security and Ransomware Protection**	**10**	• Immutable backup protection • Encryption at rest and in transit • Multi-Factor Authentication (MFA) • Role-Based Access Control (RBAC) • Privileged administrator controls • Audit trails and logging • Ransomware detection/protection • Secure deletion and retention controls	0–1 = 1 – Poor 2–3 = 2 – Fair 4–5 = 3 – Satisfactory 6–7 = 4 – Good 8+ = 5 – Excellent
4	**MANAGEMENT & REPORTING CAPABILITIES**	**10**		
4.1	**Demonstrate Management, Monitoring and Reporting**	**10**	• Real-time backup monitoring • Centralised management dashboard • Backup success/failure monitoring • Automated notifications and alerts • Backup compliance reporting • Storage utilisation and capacity reporting • Audit reports • Dashboard and report export capabilities	0–1 = 1 – Poor 2–3 = 2 – Fair 4–5 = 3 – Satisfactory 6–7 = 4 – Good 8+ = 5 – Excellent
5	**PERFORMANCE & SCALABILITY**	**10**		

5.1	**Demonstrate Backup Performance and Scalability**	**10**	• Backup throughput/performance • Recovery performance • Deduplication and compression • Impact on production systems • Storage optimisation • Ability to support future growth • Addition of servers/storage without major redesign	0–1 = 1 – Poor 2–3 = 2 – Fair 4–5 = 3 – Satisfactory 6–7 = 4 – Good 8+ = 5 – Excellent
6	**IMPLEMENTATION APPROACH**	**10**		
6.1	**Demonstrate Implementation, Migration and Transition Approach**	**10**	• Implementation methodology • Project plan and timelines • Migration from existing backup solution • Testing and acceptance approach • Cut-over approach • Rollback strategy • Risk and dependency management • Knowledge transfer and documentation	0–1 = 1 – Poor 2–3 = 2 – Fair 4–5 = 3 – Satisfactory 6–7 = 4 – Good 8+ = 5 – Excellent
7	**SUPPORT & MAINTENANCE**	**10**		
7.1	**Demonstrate Support and Maintenance Capabilities**	**10**	• 24/7 technical support • SLA and response times • Local/South African support capability • Escalation procedures • Software updates and upgrades • Preventative maintenance • Vendor/OEM support • Administrator training and knowledge transfer	0–1 = 1 – Poor 2–3 = 2 – Fair 4–5 = 3 – Satisfactory 6–7 = 4 – Good 8+ = 5 – Excellent
8	**PRESENTATION QUALITY**	**5**		
8.1	**Online Presentation and Demonstration**	**5**	• Clear and structured presentation • Live demonstration of the solution • Demonstration addresses the requirements • Vendor demonstrates technical competence • Questions answered accurately and adequately	1 = Poor 2 = Fair 3 = Satisfactory 4 = Good 5 = Excellent
	TOTAL WEIGHT	**100**		
	THRESHOLD	**70**		

6.6. Phase 4: Price and Specific Goals

6.6.1. *Preference Point System*

6.6.2. Prices quoted for all goods and services must be furnished based on supply and delivery.

6.6.3. The pricing schedule (SBD 3.3) provided in this bid forms an integral part of the bid document and bidders must ensure that it is completed without changing the structure thereof. Bidders are required to complete a mandatory Pricing Schedule as a response on how much the items offered will be charged.

6.6.4. Prices submitted for in this bid must be filled in on the field provided on the pricing schedule supplied with the bid. Price structures that do not comply with this requirement may invalidate the bid.

6.6.5. The bid prices must include all handling fees, delivery costs, and VAT.

6.6.6. The pricing evaluation will be in terms of regulation 5 of the Preferential Procurement Regulations pertaining to the Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000), responsive bids will be adjudicated by the State on the 80/20 preference point system.

6.6.7. The following formula will be used to calculate the points for price:

$$Ps = 80\left(1 - \frac{Pt - P\min}{P\min}\right)$$

Where,

Ps = Points scored for comparative price of bid under consideration

Pt = Comparative price of bid under consideration

Pmin = Comparative price of lowest acceptable bid

6.6.8. *Applicable Taxes*

6.6.8.1. All bid prices must be inclusive of all applicable taxes.

6.6.8.2. Failure to comply with this condition may invalidate the bid.

6.6.8.3. All bid prices must be inclusive of fifteen percent (15%) Value Added Tax.

6.6.8.4. Failure to comply with this condition may invalidate the bid.

6.6.9. *Points Scored for Specific Goals*

6.6.9.1. The following formula will be used to calculate the points for specific goals:

$$PSSG = MPAX\frac{POE}{100}$$

Where,

PSSG = Points scored for specific goals

MPA = Maximum points allocated for a specific goal

POE = Percentage of equity ownership by an HDI

6.6.10. *Proof of equity ownership and related matters*

6.6.10.1. The specific goals contemplated in paragraph 6.5.9.1 above must be equated to the percentage of an enterprise or business owned by individuals or, in respect of a company, the percentage of a company's

shares that are owned by individuals, who are actively involved in the management of the enterprise or business and exercise control over the enterprise, commensurate with their degree of ownership at the closing date of the tender.

6.6.10.2. In the event that the percentage of ownership contemplated in paragraph 6.5.9.1 above changes after the closing date of the tender, the tenderer must notify the Office, and such tenderer will not be eligible for any preference points.

6.6.10.3. Preference points may not be claimed in respect of individuals who are not actively involved in the management of an enterprise or business and who do not exercise control over an enterprise or business commensurate with their degree of ownership.

6.6.10.4. All claims made for specific goals must be considered according to the following criteria:

- Equity in private companies must be based on the percentage of equity ownership, and
- Preference points may not be awarded to public companies and tertiary institutions.

6.6.10.5. Equity claims for a Trust may only be allowed in respect of those persons who are both trustees and beneficiaries and who are actively involved in the management of the Trust,

6.6.10.6. Documentation to substantiate the validity of the credentials of the trustees contemplated in paragraph 6.5.10.5 above must be submitted to the Office.

6.6.10.7. A consortium or Joint Venture may claim points for specific goals, based on the percentage of the contract value managed or executed by individuals who are actively involved in the management or exercise control of the respective parties of the consortium or Joint Venture.

6.6.10.8. A tenderer must submit proof of its ownership.

6.6.10.9. A tenderer who does not submit proof of their ownership may not be disqualified from the bidding process, but they score points out of 80/20 for price and zero (0) points out of 80/20 for specific goals.

6.6.10.10. Preference points may not be claimed in respect of individuals who are not actively involved in the management of an enterprise or business and who do not exercise control over an enterprise or business commensurate with their degree of ownership.

6.6.11. *Responsive Bids*

- Bidders are required to submit responsive bids by completing all pricing on the provided pricing schedule (SBD 3.3). Non-submission of the pricing schedule (SBD 3.3) will invalidate the bid response.

6.6.12. *Specific Goals*

- The following will be used to calculate the specific goals.

a) The government intends to promote the following goals with this bid, and the points to be allocated are indicated against each goal:

Table 5: Preference Point System

#	Specific goals	Score	Required proof/ documents to be submitted for evaluation purposes
1.	**The company owned by Black people.** • 100% company owned by black people = 5 points • 75% - 99% company owned by black people = 3 points • 60% - 74% company owned by black people = 2 point • 51%- 59% company owned by black people = 1 point • 0 - 50% company owned by black people = 0 point	5 points	**Proof of claim as declared on SBD 6.1 (one or more of the following will be used verifying the tenderer's status:** • Company Registration Certification/document (CIPC) • Company Shareholders certificate • Certified identification documentation of company director/s • CSD report/ CSD registration number (MAAA number) • Agreement for a Consortium, Joint Venture, or Trust.
2.	**The company owned by Women.** • 100% company owned by women = 5 points • 75% - 99% company owned by women = 3 points • 60% - 74% company owned by women = 2 point • 51%- 59% company owned by women = 1 point • 0 - 50% company owned by women = 0 point	5 points	

#	Specific goals	Score	Required proof/ documents to be submitted for evaluation purposes
3	**The company owned by people who are Youth.** • 100% company owned by Youth = 5 points • 75% - 99% company owned by Youth = 3 points • 60% - 74% company owned by Youth = 2 point • 51%- 59% company owned by Youth = 1 point • 0 - 50% company owned by Youth = 0 point	5 points	
4	**The company owned by people who are disabled.** • 100% company owned by people who are disabled = 5 points • 75% - 99% company owned by people who are disabled = 3 points • 60% - 74% company owned by people who are disabled = 2 point • 51%- 59% company owned by people who are disabled = 1 point • 0 - 50% company owned by people who are disabled = 0 point	5 points	

b) The points scored by a bidder in respect of the goals indicated above will be added to the points scored for price.

c) Bidders are required to complete the SBD 6.1 forms in order to claim preference points. Only a bidder who has completed and signed the declaration part of the SBD 6.1 preference points claim forms will be considered for preference points.

d) The bidders must submit Identity Documents (ID), Central Supplier Database (CSD) and CIPC registration documents. These documents will serve as proof of ownership and directorship of the company.

e) Failure on the part of a bidder to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender will not be allocated with the points claimed.

f) The State may, before a bid is adjudicated or at any time, require a bidder to substantiate claims it has made about preference.

g) Points scored will be rounded off to the nearest 2 decimals.

h) If two or more bids have scored equal total points, the contract will be awarded to the bidder scoring the highest number of points for the specified goals. Should two or more bids be equal in all respects, the award shall be decided by the drawing of lots.

i) A contract may, on reasonable and justifiable grounds, be awarded to a bid that did not score the highest number of points.

j) Preference points may not be claimed in respect of individuals who are not actively involved in the management of an enterprise or business and who do not exercise control over an enterprise or business commensurate with their degree of ownership.

k) Failure on the part of the bidder to claim points for specific goals will give the bidder a score of zero (0).

PART 2: ADDITIONAL BID REQUIREMENTS

7. TERMS AND CONDITIONS

7.1. Counter Conditions

7.1.1. Bidders' attention is drawn to the fact that amendments to any of the bid conditions or setting of counter conditions by bidders may result in the invalidation of such bids.

7.1.2. The National Treasury reserves the right to change or supplement any information or to issue any addendum to this bid before the closing date and time. The National Treasury and its officers, employees and advisors will not be liable in connection with either the exercise of, or failure to exercise this right.

7.1.3. If the National Treasury exercises its right to change or supplement information in terms of the above clause, it may seek amended bid documents from all bidders.

7.2. Fronting

7.2.1. The National Treasury supports the spirit of broad based black economic empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent, and legally compliant manner. Against this background the National Treasury does not support any form of fronting.

7.2.2. The National Treasury, in ensuring that bidders conduct themselves in an honest manner will, as part of the bid evaluation processes, conduct, or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in this bid document. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade, Industry and Competition, be established during such enquiry / investigation, the onus will be on the bidder to prove that fronting does not exist.

7.2.3. Failure to do so by the bidder within a period of fourteen (14) days from date of notification by National Treasury may invalidate the bid / contract and may also result in the restriction of the bidder to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies the National Treasury may have against the bidder concerned.

7.3. Right Of Award

- The State reserves its following rights –
- Not to make any award in this bid or accept any bids submitted,
- Appoint more than one service provider(s),
- Request further technical information from any bidder after the closing date,
- Verify information and documentation of the bidder(s),
- To withdraw or amend any of the bid conditions by notice in writing to all bidders prior to closing of the bid and post award, and
- If an incorrect award has been made to remedy the matter in any lawful manner it may deem fit.

8. THIRD PARTY AGREEMENTS AND SUB-CONTRACTOR AGREEMENTS

8.1. No agreement between the bidder and any third party will be binding to the State.

8.2. In the event that bidder intends using sub-contractors to execute the Contract or part thereof, the bidder must note that it shall remain responsible and accountable for the completion of the work or delivery of services requirements.

8.3. The bidder must declare its intention to subcontract and the percentage of subcontracting thereof and must provide full description of the subcontractor.

9. SUBMISSION OF BIDS

9.1. Online bid submission

- Bidders must submit their bids online through the e-Tender Publication portal.
- Manual or hardcopy bids are not acceptable.
- The online e-Tender publication portal can be accessed on the following link: https://www.etenders.gov.za/
- The guide for online bid submission is attached as Annexure D.
- Bidders to adhere to all the rules for the online bid submission.
- Bidders' attention is drawn to the sequential submission format as per the checklist on Table 1.
- The Pricing Schedule (SDB3.3) should be submitted as such and not any other format.
- Non-compliance with online bid submission WILL invalidate the bidder's response.
- Submit all bid queries via email to NTAdminitrativetenders@treasury.gov.za.

10. COMMUNICATION AND CONFIDENTIALITY

11.1 The Financial Management Chief Directorate (FMCD) within the Office of the Director-General (ODG) may communicate with bidders where clarity is sought after the closing date and time of the bid and prior to the award of the contract, or to extend the validity period of the bid, if necessary.

10.1. Any communication to any State official or a person acting in an advisory capacity for the State in respect of this bid between the closing date and the award of the bid by the bidder is discouraged.

10.2. Whilst all due care has been taken in connection with the preparation of this bid, the National Treasury makes no representations or warranties that the content in this bid or any information communicated to or provided to bidders during the bidding process is, or will be, accurate, current, or complete. The National Treasury, and its officers, employees and advisors will not be liable with respect to any information communicated which is not accurate, current, or complete.

10.3. If a bidder finds or reasonably believes it has found any discrepancy, ambiguity, error or inconsistency in this bid or any other information provided by the National Treasury (other than minor clerical matters), the bidder must promptly notify the National Treasury in writing of such discrepancy, ambiguity, error or inconsistency in order to afford the National Treasury an opportunity to consider what corrective action is necessary (if any).

10.4. Any actual discrepancy, ambiguity, error or inconsistency in this bid or any other information provided by the National Treasury will, if possible, be corrected and provided to all bidders without attribution to the bidder who provided the written notice.

10.5. All communication between the bidder and the National Treasury office must be done in writing as per the Contact Details below.

10.6. No representations made by or on behalf of the National Treasury in relation to this bid will be binding on the National Treasury unless that representation is expressly incorporated into the contract ultimately entered between the National Treasury and the successful bidder(s).

10.7. All persons (including all bidders) obtaining or receiving this bid and any other information in connection with this bid, or the tendering process must keep the contents of the bid and other such information confidential and not disclose or use the information except as required for the purpose of developing a response to this bid.

11. CONTACT DETAILS

11.1. **Bid Enquiries:** All enquiries should be in writing to NTAdministrativetenders@treasury.gov.za. The closing date for receipt of all enquiries is 10 days before the closure of the bid. All enquiries beyond the closing date will not be considered.

12. PART 3: RECOMMENDATION AND APPOINTMENT OF BIDDERS

12.1. Once the evaluation process is complete there will be a recommendation report by the BEC to the Bid Adjudication Committee (BAC) who has the authority to either support (recommendation) or not support (recommendation) the recommendation/s to the Director General for appointment/s.

12.2. On approval of the recommendation/s and appointment/s, the successful bidder(s) will sign an acceptance letter together with the Service Level Agreement of hygiene and cleaning services for a period of Five (5) years.

12.3. Once the successful bidder has been appointed/awarded they cannot do a session to waive or cede without consultation with the department.

12.4. Consent of Information

12.4.1. By submitting a bid, the bidder consents in terms of the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA) to the State processing personal information contained in the bid (including information relating to the bidder and its directors/members/trustees/employees/agents/subcontractors, as applicable) for purposes of administering and evaluating the bid, conducting verification and due diligence (including checks with CSD, SARS, CIPC, banks, references and other third parties), concluding and managing any resulting contract, and meeting legal/governance obligations; the bidder warrants that it is authorized to provide such information and may be required to furnish additional information within a reasonable time frame determined by the department, and acknowledges the data subject rights under POPIA and that queries may be directed to the contact person in this bid document.

12.5. Tax compliance requirements

12.5.1. It is a condition of this bid that the tax matters of the successful bidder(s) are in order, or that satisfactory arrangements have been made with South African Revenue Service (SARS) to meet the bidder's tax obligations.

12.5.2. The Tax Compliance status requirements are also applicable to potential foreign bidders / individuals who wish to submit a bid.

12.5.3. It is a requirement that bidders grant a written confirmation when submitting this bid response that SARS may on an on-going basis during the tenure of the contract disclose the bidder's tax compliance status and by submitting this bid such confirmation is deemed to have been granted.

12.5.4. Bidders are required to be registered on the Central Supplier Database (CSD) and National Treasury shall verify the bidder's tax compliance status through the CSD or through SARS.

12.5.5. Where Consortia / Joint Ventures / Sub-Contractors are involved, each party must be registered on the CSD, and their tax compliance status will be verified through the CSD or through SARS.

12.6. Negotiations

12.6.1. The State reserves the right to negotiate with the shortlisted bidders prior or post award. The terms and conditions for negotiations will be communicated to the shortlisted bidders prior to invitation to negotiations. This phase is meant to ensure value for money is achieved through the measure of quality that will assess the monetary cost of the goods or services against the quality and or benefits of that goods or services.

12.7. Due diligence

12.7.1. The State reserves the right to:

- Conduct due diligence during the evaluation process to determine the ability of the bidder to honour contractual obligations that might emanate from this tendering process. The due diligence is not only limited to the bidder but to all parties the bidder might have confirmed to do business with for the fulfilment of the contract that might be awarded.
- Conduct due diligence prior to final award or at any time during the contract period and this may include pre-announced/ non-announced site visits. During the due diligence process the information submitted by the bidder will be verified and any misrepresentation thereof may disqualify the bid in whole or parts thereof.
- Conduct any evaluation verifications prior to final award or at any time during the contract term period.

END

Annexure E

Mandatory Functional Requirements Tables

1. Bidder & OEM Eligibility

Establishes that the bidder is authorised, accredited and has demonstrable relevant delivery

No.1	Mandatory Requirement	Evidence Bidder Must Provide	Compliant?
1.1	Bidder is a formally accredited partner/reseller of the proposed OEM, able to submit current, valid accreditation/partner-status certificates for both the bidder entity and the named engineers proposed for this project.	OEM partner accreditation certificate(s); named engineer certification numbers	☐ Yes ☐ No
1.2	The proposed OEM platform has to be recognized as a Leader in at least two of the following, published within the last 24 months: (a) a general backup/data-protection platform Gartner Magic Quadrant or directly equivalent report; (b) a dedicated cyber-recovery vendor assessment (e.g. an IDC MarketScape for CyberRecovery or equivalent); (c) a dataresilience Wave or equivalent. Bidder must supply report name, analyst firm, and publication date."	Published analyst report reference/extract	☐ Yes ☐ No
1.3	The proposed OEM maintains a local presence in South Africa (or committed local presence via the bidder) including support, professional services and escalation resources, not solely offshore.	Proof of local office/support desk or partner-delivered local presence	☐ Yes ☐ No

Core Platform Architecture, Immutability & Ransomware Resilience

Establishes non-negotiable minimum architecture standards for cyber-resilient data protection across National Treasury's environment.

No.	Mandatory Requirement	Evidence Bidder Must Provide	Compliant?
2.1	Solution provides a single management platform capable of protecting physical servers, virtual machines (VMware and/or Hyper-V), public cloud workloads (AWS/Azure/GCP), Network Attached Storage, databases, and Software-as-a-Service applications (including Microsoft 365) from one console and one policy engine. Vendor must confirm whether each protected workload category (data centre, cloud, Microsoft 365, identity) is licensed under the same SKU/console or requires a separately purchased and separately licensed module, and must itemise which, if any, require a separate module.	Architecture diagram; product datasheet confirming supported workload list	
2.2	The backup data store is natively immutable (append-only) by design and cannot be altered, encrypted, shortened in retention, or deleted by any user — including a fully compromised administrator account — without a documented two-person/quorum control. This control applies identically whether the action is attempted through the graphical console or the platform's API — retention-lock and quorum enforcement must not be by-passable through an API call that lacks the same two-person authorization.	Architecture whitepaper describing immutability mechanism; confirmation quorum/2-person authorisation is available	☐ Yes ☐ No
2.3	Immutability of the first backup copy does not depend on an open, network-accessible storage protocol (e.g., NFS, SMB, S3 object lock configured by the customer) that could itself be reconfigured or disabled by an attacker.	Technical architecture document describing the filesystem/protocol design	☐ Yes ☐ No

2.4	The backup software/management plane itself is proven to operate independently of, and survive compromise of, the customer's production Windows Server or hypervisor estate (i.e., the backup control plane does not run as an application on general-purpose Windows Server). Vendor must state whether the backup software's own management plane and metadata catalogue run on an OS/database maintained solely by the OEM, or on a general-purpose OS, hypervisor, or third-party database engine requiring National Treasury's own separate patch management.	Statement of backup software OS/architecture dependency	☐ Yes ☐ No
2.5	Solution includes built-in ransomware/encryption detection and IOC-based threat hunting executable directly against backup data without first restoring it, with no dependency on a third-party security tool to deliver this capability. Vendor must state the throughput of its IOC/hash-matching capability (e.g., number of backup images or terabytes screened per unit of time) and confirm whether scanning requires mounting or rehydrating the backup image.	Feature confirmation and demonstration/PoC availability	☐ Yes ☐ No
2.6	Solution can orchestrate automated, application-consistent, multi-system recovery (not only single-file/VM restore) at scale, initiated via API or a single workflow, with no manual per-system recovery steps required to bring a business application back online.	Recovery orchestration documentation; live demonstration	☐ Yes ☐ No
2.7	Bidder's proposed OEM offers a contractual ransomware recovery warranty and/or dedicated ransomware response team as part of, or available to, this contract. Vendor must disclose the maximum warranty value, whether any claim under this or an equivalent warranty has ever been paid out, and the number of ransomware recoveries its dedicated response team has supported to date, with a citation date for the figures.	Warranty terms/SLA documentation	☐ Yes ☐ No

2.8	Solution provides native sensitive-data discovery and classification capable of scanning backup data at scale (data centre, cloud and SaaS workloads) without requiring data to be restored first and without deploying endpoint agents, including a library of pre-built classifiers for common regulatory/PII data types plus the ability to define custom data types.	Feature/datasheet confirmation; list of pre-built classifiers; demonstration of scan-without-restore capability	☐ Yes ☐ No
2.9	Solution is built on an API-first architecture, such that every function available in the management console (policy/SLA creation and assignment, on-demand backup, recovery, reporting, and administration) is also exposed and fully usable through a documented, versioned API — with new features released to the API at the same time as, or ahead of, the graphical console — rather than the API being a partial or after-the-fact wrapper around the UI. Solution must provide a **documented, versioned REST API** with feature parity to the management console. Support for additional modern query interfaces (e.g., GraphQL) will be considered an advantage but is not mandatory.	Published, versioned API reference documentation (e.g., publicly accessible developer/API portal); confirmation that API coverage is at feature parity with the console, including a stated API-first release practice	☐ Yes ☐ No

2.10	Solution's API supports role-based access control equivalent to the console (i.e., a service account used for automation is bound by the same permission model as an interactive user), and supports both a modern query-based interface (e.g., GraphQL) for advanced/bulk automation and a simpler REST interface for common day-to-day operations, so both advanced automation teams and general administrators can integrate without a steep learning curve.	API authentication/RBAC model documentation; confirmation of both GraphQL and REST (or equivalent) interfaces with example requests/responses	☐ Yes ☐ No
2.11	Solution's API can be used to integrate backup, recovery, and cyber-event data directly into National Treasury's existing IT Service Management, SIEM/SOAR, and monitoring tooling (e.g., ticket creation, alert forwarding, automated on-demand snapshot or recovery triggered by an external event) without requiring professional services engagement for basic integrations.	Example integration(s) or reference architecture showing API-driven integration with ITSM/SIEM/SOAR or equivalent monitoring tooling	☐ Yes ☐ No
2.12	Solution provides an Instant/Live Mount recovery capability that presents any retained backup snapshot — a virtual machine, physical or cloud server volume, database instance, or file share — as a fully running, natively read/write workload directly from backup storage, without first copying or rehydrating the data back to production primary storage. This capability must support:	Feature/datasheet confirmation of Live Mount	☐ Yes ☐ No

	(i) near-instant application availability during a ransomware or disaster recovery event; (ii) non-disruptive recovery/DR testing against production-representative data without impacting live production systems or consuming primary storage capacity; and (iii) mounting a snapshot into an isolated, network-segmented environment for malware-free validation of a recovery point before it is promoted to production Vendor must state the maximum number of concurrent VMs or servers that can be brought online via this mechanism within a single orchestrated recovery operation, and the average time-to-availability for a single workload.	(or equivalent) capability; demonstration of instant, direct-from-backup-storage availability with no prior data-copy/rehydration step, across VM, database and file workloads	
2.13	Solution provides native, vendor-built integration with Microsoft Defender (e.g., Microsoft Defender XDR, Defender for Cloud, Defender for Endpoint) enabling security alerts and threat intelligence to be ingested directly into the data protection platform and correlated against backup and recovery data and workflows — not via a generic, customer-built API script or a third-party SIEM as a mandatory intermediary. Solution must support **standards-based integration** with Microsoft security tooling (including Microsoft Defender and Microsoft Sentinel) using documented APIs, connectors, or Common Event Format/Syslog, enabling correlation of backup-platform events alongside identity and endpoint signals in a single SOC view. Native vendor-provided connectors will be considered an advantage but are not mandatory.	Feature/datasheet confirmation of native Microsoft Defender integration; description of alert-ingestion and threat-correlation workflow	☐ Yes ☐ No

2.14	Solution can forward security-relevant events generated by the data protection platform — including ransomware/encryption-detection alerts, anomaly and identity-drift alerts, backup/recovery job status, and audit events — into Microsoft Sentinel, either via a native, vendor-supported connector or a standards-based method (e.g., Common Event Format over Syslog, a documented REST API, or a Sentinel Logic App/Data Connector), so National Treasury's security operations team can correlate backup-platform events alongside Microsoft Defender and Entra ID Protection signals in a single Sentinel workspace without custom, bidder-specific development work.	Feature/datasheet confirmation of Microsoft Sentinel integration or supported ingestion method (connector, CEF/Syslog, REST API, or Logic App/Data Connector); sample event schema showing the event types forwarded	☐ Yes ☐ No

3. Microsoft 365 (SaaS) Data Protection & Microsoft Relationship

Given the shared-responsibility model (Microsoft does not guarantee recovery of M365 data), the following are mandatory minimums for any solution proposed to close this gap.

No.	Mandatory Requirement	Evidence Bidder Must Provide	Compliant?
3.1	Bidder's proposed OEM must demonstrate a formal, documented engineering or strategic relationship with Microsoft specific to the protection of Microsoft 365 data (Exchange Online, SharePoint Online, OneDrive, Teams) — e.g., joint engineering programme, named Microsoft partnership status, or Microsoft as a disclosed investor/strategic partner in the OEM. A generic "Microsoft Certified Partner" badge alone does not satisfy this requirement.	Signed letter or published documentation evidencing the specific relationship, dated within the last 12 months	☐ Yes ☐ No

3.2	Solution stores an immutable, air-gapped copy of Microsoft 365 data outside of National Treasury's own Microsoft 365/Azure tenant, distinct from native Recycle Bin, Versioning, Retention Hold, or Litigation Hold.	Architecture confirmation of storage location and isolation model	☐ Yes ☐ No
3.3	Solution provides a prioritised, large-scale recovery workflow for Microsoft 365 data capable of recovering specific users/critical data ahead of others during a mass-recovery cyber event, not a manual, one-object-at-a-time restore.	Recovery workflow documentation/demonstration	☐ Yes ☐ No
3.4	Solution provides native sensitive data discovery and classification across Microsoft 365 services, with the ability to complement Microsoft Purview labelling and to support safe use of the data by AI tools such as Microsoft 365 Copilot.	Feature confirmation; list of pre-built data classifiers	☐ Yes ☐ No
3.5	Solution protects Microsoft 365 under the same policy engine, retention framework and console as the bidder's proposed datacentre and cloud protection (single platform), rather than as a disconnected, separately licensed and separately managed point product.	Confirmation of unified console/platform for M365 and other workloads	☐ Yes ☐ No
3.6	Solution provides comprehensive coverage across Exchange Online (mail, calendar, contacts), SharePoint Online (sites, lists, libraries), OneDrive for Business, and Microsoft Teams (chat, channel messages, and files), backed up on independently configurable schedules per workload/service.	Datasheet/feature matrix confirming per-service M365 coverage and scheduling granularity	☐ Yes ☐ No
3.7	Solution provides global, cross-service search and granular object-level recovery (e.g., a single email, file, Teams message, or SharePoint list item) without requiring recovery of the entire mailbox, site, or drive.	Demonstration of granular/global search and recovery capability	☐ Yes ☐ No
3.8	Solution enforces credential isolation for administrative access to the M365 backup environment (e.g., dedicated authentication separate from the customer's own M365 tenant credentials, with MFA/TOTP required), so that a compromise of the customer's M365 admin credentials does not automatically grant access to the M365 backup data. Vendor must disclose any historical security incident in which customer Microsoft 365 authentication tokens or credentials were compromised via the backup platform itself, and the remediation taken.	Security architecture documentation describing credential/authentication isolation for M365 protection	☐ Yes ☐ No

3.9	Solution licensing for Microsoft 365 protection is per-seat/user based, with no separate per-GB storage penalty that would cause costs to escalate unpredictably as mailbox/OneDrive/SharePoint data grows.	Commercial/licensing model confirmation for M365 protection	☐ Yes ☐ No
3.10	[Not mandatory — scored as value-add, not pass/fail.] Solution can extend or integrate with Microsoft 365 Backup Storage (where the customer has it enabled) rather than operating as a fully disconnected, duplicate backup silo for the same data. Where Microsoft 365 Backup Storage is enabled, the solution **should be able to coexist or integrate** using standard APIs or supported methods. This will be evaluated as a desirable capability rather than a mandatory requirement.	Architecture/integration documentation confirming interoperability with Microsoft 365 Backup Storage	☐ Yes ☐ No

4. Microsoft Identity Resilience (Entra ID & Active Directory)

Identity systems are now among the most targeted components in cyberattacks; the following are mandatory minimums for any solution proposed to close this gap.

No.	Mandatory Requirement	Evidence Bidder Must Provide	Compliant?
4.1	Solution provides native backup and recovery of Microsoft Entra ID (Azure AD) beyond the native 30-day recycle bin, explicitly including Enterprise Applications, App Registrations, and Conditional Access Rules — not limited to users, groups and roles only.	Feature/datasheet confirmation of Entra ID object coverage	☐ Yes ☐ No
4.2	Solution provides native, forest-level Active Directory backup and recovery, distinct from VM-level snapshot backup (which forces a full clean OS rebuild) or manual/scripted software-level recovery.	Architecture documentation describing AD Forest recovery method	☐ Yes ☐ No
4.3	Solution can recover an entire Active Directory Forest into an isolated clean-room environment (new, clean infrastructure) to prevent reinfection during a cyber recovery, without dependency on the compromised production domain.	Clean-room recovery process documentation/demonstration	☐ Yes ☐ No
4.4	Solution orchestrates recovery across hybrid identity environments (on-premises Active Directory and Entra ID) from a single platform and a single recovery plan, maintaining consistency of identity objects across both, rather than requiring two separate point products run independently of one another.	Architecture confirmation of unified hybrid identity recovery	☐ Yes ☐ No

4.5	Solution is aware of, and correctly handles, the synchronisation relationship between on-premises Active Directory and Entra ID (e.g., via Microsoft Entra Connect/Azure AD Connect), including distinguishing hard-matched from soft-matched objects, so that a recovery does not create duplicate, orphaned, or conflicting identity objects once directory synchronisation resumes.	Architecture/technical documentation describing directory-synchronisation awareness during recovery; demonstration or PoC evidence	☐ Yes ☐ No
4.6	Solution allows the customer to define and control the recovery sequence across the hybrid identity estate (e.g., recovering on-premises Active Directory first, then reconciling with Entra ID, or another customer-defined runbook order), rather than forcing a single fixed recovery order.	Documentation confirming configurable recovery sequencing across AD and Entra ID	☐ Yes ☐ No
4.7	Following a hybrid identity recovery, solution provides a validation/reconciliation report confirming consistency of identity objects, group memberships, and attributes between the recovered on-premises Active Directory and Entra ID, to give assurance the hybrid identity estate is in a known-good state before business services are reopened.	Sample post-recovery validation/reconciliation report or feature confirmation	☐ Yes ☐ No
4.8	Solution captures and securely escrows BitLocker recovery keys for domain controllers and other BitLocker-encrypted identity infrastructure independently of Active Directory itself, so that BitLocker-encrypted domain controllers can be decrypted and recovered even when the Active Directory environment that would normally store those recovery keys is itself unavailable or destroyed (avoiding a circular recovery dependency).	Architecture/technical documentation describing independent BitLocker recovery-key capture, storage, and retrieval process; demonstration of decrypting a BitLocker-protected domain controller during a forest recovery scenario	☐ Yes ☐ No
4.9	Solution provides continuous monitoring and alerting of unauthorised or anomalous changes to identity objects and attributes (identity drift/privilege escalation detection).	Feature confirmation/demonstration	☐ Yes ☐ No
4.10	Retention of identity backups is configurable and not capped at a fixed native platform limit (e.g., 30 days), to cover realistic attacker dwell times.	Retention policy documentation	☐ Yes ☐ No

4.11	Solution provides native integration with Microsoft Defender for Identity (and/or Entra ID Protection), ingesting identity-threat alerts directly into the platform and automatically correlating all activity performed by a compromised identity across both on-premises Active Directory and Entra ID using an identity activity log. Following correlation, an administrator must be able to either cherry-pick and revert only the specific malicious changes or bulk-revert all attacker actions, preserving legitimate changes made in the same period rather than performing a blind rollback — delivered as a single Detection → Correlation → Recovery workflow rather than as separate, manually-stitched-together tools.	Feature/datasheet confirmation of Microsoft Defender for Identity (or Entra ID Protection) integration; description of activity correlation and selective/bulk-revert capability; demonstration of the Detection → Correlation → Recovery workflow	☐ Yes ☐ No

5. Zero-Trust Security & Access Control

No.	Mandatory Requirement	Evidence Bidder Must Provide	Compliant?
5.1	Multi-factor authentication (MFA) is enforced by default for all administrative access and cannot be disabled by a local administrator.	Security architecture documentation	☐ Yes ☐ No
5.2	Solution enforces quorum/two-person authorisation for high-risk actions such as retention-period changes or mass deletion.	Security/RBAC documentation	☐ Yes ☐ No
5.3	Solution's time source for retention enforcement is resistant to manipulation (e.g., not solely reliant on a network time protocol that can be spoofed/poisoned). Vendor must describe how retention-lock timing has been validated against network time manipulation attempts (e.g., through independent testing, red-team exercise, or a documented real-world incident and its outcome).	Architecture documentation describing time-source mechanism	☐ Yes ☐ No

6. Implementation, Support & Skills Transfer

No.	Mandatory Requirement	Evidence Bidder Must Provide	Compliant?
6.1	Bidder provides a documented implementation methodology and project plan, OEM resources for this engagement.	Project plan; CVs and accreditation of named resources	☐ Yes ☐ No

6.2	Bidder commits to a structured skills- and knowledge-transfer programme to National Treasury staff, including a defined certification pathway.	Skills transfer plan and training curriculum	☐ Yes ☐ No
6.3	Bidder provides premium support with defined severity-based response and resolution SLAs.	Support SLA documentation	☐ Yes ☐ No

7. Commercial & Total Cost of Ownership Transparency

No.	Mandatory Requirement	Evidence Bidder Must Provide	Compliant?
7.1	Pricing model is consumption/capacity-based and does not require forklift hardware upgrades as data volumes grow within the contract period.	Pricing model description; scalability cost statement	☐ Yes ☐ No
7.2	All licensing, maintenance, support and future scalability costs are itemised transparently for the full contract period, with no undisclosed cost categories.	Fully itemised commercial schedule	☐ Yes ☐ No

8. Bidder Declaration

We, the undersigned, confirm that the proposed solution meets **ALL** the mandatory requirements listed in Sections 1–7 above, and that the evidence attached in support of each item is true and accurate. We understand that any misrepresentation discovered during due diligence, proof-of-concept, or contract implementation will render this bid disqualified and may result in further legal consequence in terms of the applicable procurement legislation.

Bidder Company Name: _____

Authorised Signatory: _____

Designation: _____

Date: _____