

REQUEST FOR PROPOSAL FOR THE APPOINTMENT OF A SERVICE PROVIDER FOR SACN ENTERPRISE STORAGE BACKUP AND RECOVERY

ISSUED DATE: 13 October 2026

CLOSING DATE AND TIME: 28 October 2026 at 17:00 PM.

METHOD OF SUBMISSION AND ENQUIRIES

All proposals and enquiries must be submitted via email to the email address specified in this RFP. No other method of submission will be accepted.

TABLE OF CONTENTS

1. BACKGROUND	3
2. PURPOSE OF THE ASSIGNMENT	3
3. OBJECTIVES	3
4. SCOPE OF WORK	3
5. PRIORITY STORAGE REQUIREMENTS	4
6. NETWORK POWER AND SECURITY REQUIREMENTS	6
7. BACKUP REPLICATION AND RECOVERY	7
8. MONITORING AND MAINTENANCE	8
9. WORKING ARRANGEMENT	9
10. DELIVERABLES	9
11. BUDGET AND COST CONTROL	10
12. RECOMMENDED BUDGET STRUCTURE	10
13. CONTRACT MANAGEMENT AND APPROVALS	11
14. EXPECTED TURNAROUND TIMES	11
15. REPORTING	12
16. KEY PERFORMANCE INDICATORS	12
17. REQUIRED EXPERIENCE AND CAPACITY	13
18. PROPOSED TEAM	13
19. PROPOSAL REQUIREMENTS	14
20. EVALUATION AND SELECTION CRITERIA	15
21. CONTRACT PERIOD	18
22. ASSUMPTIONS AND EXCLUSIONS	18
23. INTELLECTUAL PROPERTY AND CONFIDENTIALITY	18
24. VALUE FOR MONEY	19
25. SUBMISSION	19
26. ANNEXURES	20
Annexure A Testing and acceptance schedule	20

1. BACKGROUND

The South African Cities Network (SACN) is a knowledge and learning network that supports good governance and management in South African cities through research, evidence, partnerships and shared learning.

SACN requires reliable access to its organisational files and dependable recovery of those files when equipment fails, information is deleted or corrupted, or a security incident occurs. Centralised storage and independently protected backup copies will support daily operations and business continuity.

2. PURPOSE OF THE ASSIGNMENT

Appointment of a service provider to supply, install, configure and commission an enterprise storage and data protection solution, including migration, training and 24 months of monitoring and operational support.

1. SACN requires centralised organisational file storage with controlled access, sufficient growth capacity and dependable recovery. The appointment must deliver a fully commissioned solution that separates live data from recoverable copies and reduces exposure to equipment failure, accidental deletion, ransomware and site disruption.

The appointment covers once-off implementation and 24 months of monitoring and operational support from formal acceptance, with a minimum 36-month hardware warranty and support period.

3. OBJECTIVES

- Consolidate agreed organisational file data into a controlled central storage service.
- Apply departmental access permissions, encryption and auditable administration.
- Maintain independent backup and protected off-site recovery copies.
- Migrate data without unexplained loss and prove restoration through witnessed tests.
- Provide sufficient operational headroom, transparent growth planning and complete licensing.
- Enable SACN administrators to operate the solution through training and documented procedures.

4. SCOPE OF WORK

4.1 Overall storage and backup services

- Assess existing data sources, directory services, network capacity, rack space, power, connectivity and recovery priorities; submit a final design and capacity model.
- Supply one enterprise primary storage system and one physically separate enterprise backup system, complete with storage software, drives, rails, cables and all required licences.
- Provide protected off-site backup capacity, network integration and correctly sized UPS protection; include every dependency needed to achieve the contracted outcomes.
- Integrate with SACN's existing directory service; create approved departmental shares, group permissions, quotas and audit logging.
- Migrate the agreed file datasets; preserve permissions, timestamps and ownership where supported; record and resolve exceptions with the data owners.
- Configure backup schedules, immutable or offline protection, alerts and recovery procedures; test and document the complete solution.

- Provide administrator training, handover records and 24 months of monitoring, corrective support, reporting and scheduled restore testing.

4.2 Vendor neutrality and compliance

All makes and supported architectures meeting the functional and performance requirements may be offered. References to existing protocols or directory services describe interoperability, not a preferred supplier. Brand, processor model, country of origin or a proprietary feature name shall not substitute for evidence of compliance.

Requirements stated as "must", "shall" or "minimum" are mandatory once this TOR is approved. Bidders must identify every deviation. An alternative architecture may be submitted separately with a requirement-by-requirement equivalence case, complete pricing and measurable outcomes; it may not silently replace the compliant base offer.

Technical and service requirements are detailed in Sections 5 to 8. Deliverables, service times, reporting and acceptance are addressed in Sections 10 and 14 to 16 and Annexure A.

5. PRIORITY STORAGE REQUIREMENTS

The base solution must include one primary storage system and one physically separate backup repository. The agreed storage capacities are set out below; actual formatted capacity must be disclosed.

Primary storage	Backup repository	Data protection
48 TB raw (6 × 8 TB) ≈32 TB usable after RAID 6* 64 GB ECC memory	64 TB raw (4 × 16 TB) ≈32 TB usable after RAID 6* 64 GB ECC memory	10GbE connectivity Protected off-site copy Tested recovery procedures

* Usable RAID capacity is stated before file-system overhead and system reserves. Actual formatted capacity will be lower. Both servers include 2 × 480 GB boot SSDs, separate from the data capacity above.

5.1 Primary storage platform

Component	Minimum requirement
Platform	New, unused, enterprise rack-mounted storage server or NAS appliance suitable for continuous operation in a standard 19-inch rack. Include rails and cable management. State rack height, depth, weight and ventilation needs.
Processing	Server-class 64-bit processor(s), minimum 16 physical cores in total, hardware-assisted encryption and ECC support. State processor generation and performance evidence for the proposed workload.
Memory	64 GB installed ECC RAM (2 × 32 GB); expandable to at least 128 GB without replacing the platform. State populated slots, maximum capacity and upgrade method.
Data capacity	48 TB installed raw data capacity using 6 × 8 TB enterprise drives in RAID 6, providing approximately 32 TB usable after parity and before file-system overhead and system reserves. Exclude boot drives and spare drives from these figures.

Component	Minimum requirement
Drive protection	Enterprise CMR HDDs and/or enterprise SSDs rated for the proposed workload and supported by the platform. RAID 6, dual-parity software RAID, or equivalent tolerance of any two data-drive failures per protection group. No single-parity configuration.
Boot and resilience	Two enterprise SSD boot devices of at least 480 GB each in a mirrored arrangement, or an equally resilient supported boot design. Hot-swappable data drives, redundant hot-swap power supplies and resilient cooling. One compatible on-site spare data drive included.
Connectivity	At least two 10GbE data ports and dedicated out-of-band management, or a functionally equivalent isolated management interface. Include management feature licences and matched optics/DACs/cables.
File services	SMB 3.1.1; directory-based authentication; granular group ACLs; quotas; snapshots; previous-version recovery; usage reporting and administrative audit logs. NFS capability may be offered where required.
Expansion	A supported path to at least double the delivered net capacity using additional drives or expansion shelves. Explain downtime, licences and any controller limits; price expansion units separately.
Supportability	OEM or accountable platform vendor support, security updates and replacement parts for at least 36 months from acceptance. No end-of-support equipment or grey-market components. State all announced lifecycle dates.

TB means 10^{12} bytes; report TiB and actual formatted capacity separately. The approximately 32 TB RAID capacity is before file-system overhead and system reserves, not a guaranteed net allocatable minimum. Model 20% operational free space through month 24, including snapshots. Identify and separately price any expansion required for SACN approval; retain the 48 TB raw base configuration.

The bidder must state sustained throughput with encryption and protection enabled, including concurrent file use and backup activity. Acceptance performance is set out in Annexure A; nominal interface speed alone is not proof of storage performance.

5.2 Independent backup platform

Component	Minimum requirement
Separation	Physically separate rack-mounted backup server or appliance. A volume, virtual machine or partition on the primary storage system is not an independent backup repository.
Compute	Minimum 12 physical server-class processor cores and 64 GB ECC RAM (2 × 32 GB), expandable to at least 128 GB. An appliance with different internals must demonstrate equivalent ingest, verification and recovery performance.
Repository capacity	64 TB installed raw data capacity using 4 × 16 TB enterprise drives in RAID 6, providing approximately 32 TB usable after parity and before file-system overhead and system reserves. Boot disks, spare disks and any live recovery workspace are excluded.

Component	Minimum requirement
Hardware resilience	Hot-swappable enterprise CMR HDDs and/or enterprise SSDs; any-two-drive fault tolerance per protection group; mirrored boot SSDs of at least 480 GB each or equivalent resilient boot; redundant hot-swap power and cooling; one on-site spare data drive.
Networking	At least two 10GbE ports with complete interconnects and isolated management. Restrict repository ingress to authorised backup services and management paths.
Backup software	Automated full/synthetic-full and incremental backup, versioned retention, encrypted transfer, catalogue protection, integrity verification, granular file and full-share restoration, scheduling, alerting and exportable reports.
Protected recovery points	Implement an immutable repository or an offline/air-gapped copy with documented protection from production administrator compromise. Ordinary file permissions or source snapshots alone do not meet this requirement.
Independent administration	Separate backup administrative credentials and trust boundary. Routine production/domain administrators must not be able to delete all retained recovery copies. Provide audited, controlled break-glass access.
Recovery portability	Restore file data and permissions to an alternative supported target. Document catalogue rebuild, key recovery and recovery without the original primary system or normal directory service being available.
Lifecycle	Minimum 36-month hardware support and 24-month software maintenance/subscriptions. State behaviour after subscription expiry and costs needed to retain recovery access.

Calculate the protected dataset, growth, daily change rate, retention, full-backup strategy, immutable overlap, metadata and 20% free space through month 24. Show achievable retention without assumed data reduction, with any evidenced savings separately. Retain the 64 TB raw base repository; price any capacity shortfall separately for SACN approval before issue or award.

Approximately 32 TB of backup RAID capacity does not guarantee 90 days of history. Target up to 90 days for critical data, subject to actual data volume and change rate. Confirm the achievable schedule and any separately priced expansion before commitment.

6. NETWORK POWER AND SECURITY REQUIREMENTS

6.1 Network integration

- Provide an end-to-end 10GbE path between the supplied systems. Inspect existing switch capacity and interoperability; include all necessary ports, optics, cables and configuration.
- Provide redundant data paths. Where resilient existing switches cannot be reused, include two suitably sized managed switches with 10GbE uplinks, VLANs, link failover, monitoring and supported firmware.
- Separate user, backup and management traffic using VLANs and access controls. Document firewall flows and prohibit direct public exposure of storage and management interfaces.
- Validate client and WAN bottlenecks. Link aggregation must not be represented as doubling the speed of a single client transfer. Cost required WAN changes separately and state achievable off-site transfer times.

6.2 UPS and electrical integration

Provide online double-conversion UPS protection, nominally at least 3 kVA for a shared installation, with sufficient output watts for the servers and associated supplied network equipment. Keep the projected load at or below 80% of the UPS watt rating and demonstrate at least 15 minutes of runtime at the actual configured load. Include additional batteries where needed.

If systems occupy separate sites or power zones, size and include UPS protection for each unless SACN confirms that an existing unit satisfies the same criteria. Include monitoring, battery alarms, controlled shutdown, safe restart sequencing, rails and appropriate power connections. Submit OEM runtime curves and an on-site load test. A shared UPS is a common failure point; disclose it and price A/B power resilience separately where unavailable.

6.3 Identity and platform protection

- Integrate production file access with SACN's existing Active Directory or approved directory service. Apply least-privilege group access, disable guest access and avoid routine use of domain-administrator accounts.
- Use separate named administration accounts, MFA for privileged consoles and remote access, and a controlled management gateway where native MFA is unavailable. Log privileged actions and periodically review access.
- Enable SMB 3 encryption for sensitive shares and all backup transfers. Require signing for unencrypted SMB sessions; encrypted SMB provides its own integrity protection. Disable SMB1 and unsupported legacy protocols. Validate client compatibility before cutover. [2]
- Encrypt stored production and backup data using AES-256 or an equivalent approved mechanism; use supported encrypted management and transfer protocols. Provide SACN with controlled key custody, escrow/recovery procedures and a tested key-recovery path.
- Harden the operating system, firmware and management interfaces; remove default credentials and unnecessary services. Use secure boot and hardware trust facilities where supported. Maintain a supported patch baseline and approved maintenance windows.
- Export audit and security logs to a protected destination; retain at least 90 days online and 12 months in searchable archive. Log access changes, administrative actions, job status and retention/deletion changes; exclude secrets from reports.

7. BACKUP REPLICATION AND RECOVERY

7.1 Backup schedules and retention

- Automated daily incremental backups with a weekly full or synthetic-full strategy, or an equivalent demonstrably recoverable chain. Backups must complete within an 8-hour nightly window at the stated sizing baseline.
- For designated critical file data: recovery points at least every 4 hours during 08:00-17:00 SAST, Monday-Friday excluding public holidays, plus a daily independent backup. Identify whether each point is a snapshot, local backup or off-site backup.
- Target up to 90 days of daily recovery points for critical data, subject to actual volume and daily change rate. Model 30 days for other data and the off-site copy. Confirm achievable retention within the base capacity before issue; separately price any expansion needed for SACN approval.

- At least one independent copy must be immutable or physically offline for a minimum of 30 days. Retention locks must not be reducible by a compromised production administrator. Explain privileged override risks and controls.
- Verify completed jobs automatically; check backup-chain integrity at least weekly. Alert on failure, missed schedules, stale recovery points, lock changes and capacity thresholds. Retry failures and escalate before the applicable RPO is exceeded.
- Restore deleted, corrupted and older file versions with permissions and relevant metadata. Scan recovered content where appropriate before reintroducing it into production. Retain evidence of recovery tests.

7.2 Protected off-site copies

The mandatory base offer must include an off-site recovery copy in addition to production data and the local backup copy. Use an immutable object-storage service, an offline tape/media rotation service, or an equivalent independently protected system. Deliver three recoverable copies overall, at least two independent storage technologies or protection domains, one off-site copy and one immutable or offline copy.

- Use a location outside the primary site's physical risk boundary. A different rack in the same room does not count as off-site.
- Encrypt off-site copies and implement separate administrative control. State the location, custody arrangements, service provider, retention, deletion controls and key ownership.
- Include 24 months of capacity, licences, transfer, media handling, routine testing and one full-dataset recovery/export event at the disclosed sizing baseline. Disclose overage and additional recovery charges.
- Default hosting and media custody must be in South Africa. Any alternative location requires SACN's written approval and an assessment of applicable data-transfer obligations before use.

Copy separation, retention locks and recovery tests must be demonstrated. Mirroring or replication that immediately propagates deletion or corruption is not sufficient on its own.

7.3 Recovery objectives

Scenario	RPO / maximum data loss	RTO / restore target
Accidental deletion; primary healthy	4 business hours for critical files; 24 hours for other files	≤1 hour for an agreed file/folder set up to 10 GB
Primary system unavailable	≤24 hours using the independent repository	Priority dataset up to 1 TB: ≤8 hours; all in-scope file data: ≤48 hours
Primary site unavailable	≤24 hours using the off-site copy	Priority dataset up to 1 TB: ≤72 hours at the agreed alternate recovery location

RPO is the maximum age of the last recoverable copy at the incident. RTO runs from SACN's authorised recovery declaration until usable service is restored, including preparation, key access and transfer. The 1 TB priority dataset is a tender sizing assumption, not a statement of SACN's current volume. SACN must confirm the priority data and alternate location before issue.

Include the temporary storage/compute, recovery workspace and connectivity necessary to meet the targets. Any dependency on replacement hardware, third-party access or bandwidth must be priced and

evidenced. Bidder exceptions require explicit evaluation; targets may not be reduced unilaterally after award.

Operational backup retention does not replace SACN's records-retention policy. Confirm legal holds, permitted deletion and any archive requirement with the relevant data owners.

8. MONITORING AND MAINTENANCE

Provide automated 24×7 health and backup monitoring, with 24×7 human response to Priority 1 incidents. Routine support hours are 08:00-17:00 SAST, Monday-Friday excluding South African public holidays. The contract must include remote corrective action and necessary on-site support at the disclosed locations; attendance/travel assumptions must be stated in the offer.

- Review failed jobs and storage alerts each business day; monitor disk health, temperature, power, capacity, replication lag, retained points and immutable-copy status. Use warning/critical capacity thresholds of 70%/80%, adjustable with SACN approval.
- Perform monthly sample file restores, quarterly priority-dataset recovery exercises and an annual end-to-end recovery exercise, including an off-site recovery scenario. Record elapsed recovery time and defects; remediate failed tests.
- Review patches monthly. For actively exploited or critical vulnerabilities, provide a mitigation plan within one business day of notification; implement approved mitigation promptly and track final remediation.
- Check support entitlements, batteries, spare-drive readiness and growth forecasts. Preserve configuration backups after approved changes; document changes and rollback steps.

Incident priorities and response commitments are set out in Section 14.2. Monthly operational reporting and quarterly reviews are required under Section 15.

9. WORKING ARRANGEMENT

9.1 Coordination and responsibilities

The appointed provider will work with SACN's designated ICT representative and relevant departmental data owners. SACN will provide approved access to sites, systems and source data; nominate an ICT lead and data owners; and coordinate user communications, maintenance windows and approvals.

The provider must maintain a project plan, dependency register, change record and escalation contacts. All bidders must receive the same confirmed workload and site information.

9.2 Migration safeguards

- Identify the authoritative source and obtain an approved migration manifest. Check file counts, sizes, ACLs, long paths, locked files and unsupported metadata; document exceptions before cutover.
- Take a verified pre-migration recovery copy. Pilot representative folders; perform staged bulk and final-delta copies within approved maintenance windows.
- Validate file counts and byte totals and hash-check critical data and an agreed representative sample. Obtain data-owner checks for access and usability.
- Keep the original source protected and available for rollback until SACN signs acceptance and separately authorises disposal. Do not delete source data as part of routine cutover.

10. DELIVERABLES

Workstream	Required deliverables
Assessment and design	Site-readiness assessment, source-data inventory, architecture, bill of materials, capacity and retention calculations, risk register and approved implementation plan.
Storage and backup platforms	Commissioned primary system and separate backup repository, protected off-site copy, complete networking and UPS integration, and registered support entitlements.
Migration and access	Approved migration manifest, departmental shares, permissions matrix, validation evidence and rollback records.
Testing and commissioning	Completed acceptance register, security and resilience tests, recovery evidence and resolved defects in accordance with Annexure A.
Handover and support	Editable operational documentation, administrator training, configuration records, monthly reports and recovery-test records.

10.1 Documentation and training

Deliver as-built network and storage diagrams; serial/asset registers; licences and warranties; capacity calculations; configuration exports; permissions matrix; backup and retention policy; test results; monitoring thresholds; escalation contacts; and step-by-step recovery, shutdown, restart and patching procedures. Transfer credentials and keys through a secure channel, separate from the report.

Provide at least two practical administrator sessions of two hours each for up to four SACN nominees, covering normal operations and supervised restoration. Supply editable guides and attendance records.

11. BUDGET AND COST CONTROL

Price the complete mandatory base solution. State VAT registration status and show VAT separately only where applicable; a non-VAT-registered bidder must state that status. Do not assume that SACN will fund omitted licences, interfaces or recovery capacity.

SACN will approve the contract value and any applicable procurement budget before award. Bidders must provide a complete and transparent price for the mandatory solution and identify every dependency. Hardware, implementation, licensing, recurring support, off-site capacity and third-party charges must be distinguishable.

- State quotation validity (proposed minimum 60 days), delivery lead time, payment milestones, currency/exchange assumptions and any escalation formula.
- Disclose protected-capacity limits, excess TB charges, restore/egress fees beyond included allowances, travel, after-hours terms and year-three software/support renewal estimates.
- Separately price optional high-availability clustering, A/B UPS resilience, extended retention, extra capacity and years four/five of support. Do not include options in the base total.
- If reusing SACN equipment, identify the asset and confirmed capability and show the dependency/reuse credit. A dependency that has not been confirmed must also have a priced supply option.

No third-party expenditure, additional capacity, licence upgrade, travel outside the agreed allowance or change to the approved scope may be committed without SACN's prior written approval. Any approved budget ceiling must be applied consistently to all bidders.

12. RECOMMENDED BUDGET STRUCTURE

The financial proposal must distinguish once-off supply and implementation from the 24-month managed service and any separately priced options. Hardware support must cover at least 36 months. Quote all amounts in South African rand and avoid double-counting bundled items.

Item	Qty / basis	Once-off / 24-month amount
1 - Primary storage system, drives, spare and rails	1 complete system	R _____
2 - Backup system, drives, spare and rails	1 complete system	R _____
3 - Required network switches and interconnects	Per final design	R _____
4 - UPS units, batteries and management	Per site/load design	R _____
5 - Storage/backup licences and maintenance	24 months; state metric	R _____
6 - Protected off-site copy and transfer/recovery allowance	24 months; state TB baseline	R _____
7 - Design, installation, migration and commissioning	Fixed fee	R _____
8 - Training, documentation and acceptance tests	Fixed fee	R _____
9 - Monitoring, corrective support and reporting	Monthly rate × 24	R _____
10 - Hardware warranty / OEM support	36 months; avoid double-counting	R _____
11 - Required recovery workspace and other dependencies	Itemise; no undisclosed exclusions	R _____
A - Total mandatory base cost, excluding VAT	Sum items 1-11	R _____
B - VAT, where applicable	Rate / amount or not applicable	R _____
C - Total mandatory base cost, including applicable VAT	A + B	R _____

State the base capacity and consumption assumptions, monthly recurring charge, full 24-month total, renewal costs and all exclusions. Optional enhancements must remain outside the mandatory base total unless approved by SACN.

13. CONTRACT MANAGEMENT AND APPROVALS

SACN's authorised representative must approve the detailed design, migration and rollback plan, maintenance windows, material changes and final acceptance. The provider must obtain written approval before substituting any quoted model or changing the agreed scope, retention or recovery objectives.

SACN's authorised ICT representative shall sign an acceptance certificate supported by the test register and outstanding-items list. Critical or high-impact defects prevent acceptance. Minor items require written owners and dates. Delivery, installation or routine use alone shall not be treated as acceptance. The provider must correct failed tests and repeat affected tests at no additional cost.

Final payment terms will be set by SACN and linked to delivery, commissioning and acceptance. Any requested advance payment must be disclosed and supported by the security arrangements required by SACN's policy. No deposit percentage is prescribed in this RFP.

Maintain a record of approved changes, costs, dependencies and decisions. The provider remains accountable for subcontracted services and must resolve failed acceptance tests at no additional cost.

14. EXPECTED TURNAROUND TIMES

14.1 Implementation programme

Phase / target	Required deliverable and release gate
1 - Discovery Within 5 business days of commencement	Inventory; site readiness; data volume/change rate; migration sources; directory compatibility; risk and dependency register. SACN confirms scope and owners.
2 - Detailed design Within 10 business days of commencement	Architecture; bill of materials; capacity/retention model; permissions matrix; security design; migration, rollback and acceptance plans. SACN approves before deployment.
3 - Procurement Indicative 15-25 business days	Bidders must commit lead times and disclose stock constraints. Provide authorised-channel evidence, exact part numbers and support registration. Any substitution requires prior written approval.
4 - Installation and migration Indicative 5-10 business days after delivery and readiness	Rack, power and network installation; hardening; storage and backup configuration; migration pilot; staged copy; validation; approved cutover. Duration must be justified against data volume and throughput.
5 - Stabilisation and acceptance 10 consecutive business days after cutover	Operational monitoring, resolved critical defects, all acceptance evidence, administrator training and signed handover. The 24-month service period begins at formal acceptance.

14.2 Incident response and restoration

Priority / example	Response	Action and communication
P1 - Storage unavailable; suspected compromise; no usable protected copy	≤1 elapsed hour, 24×7	Start remediation within 2 elapsed hours; update hourly; restore to the Section 7.3 targets. Escalate to SACN immediately for security incidents.
P2 - Degraded protection; failed backup with a valid prior copy; redundancy lost	≤4 support hours	Workaround/action plan within 1 business day; daily updates. Escalate to P1 if RPO is breached or all protected copies are at risk.

Priority / example	Response	Action and communication
P3 - Routine request, capacity trend or non-critical defect	≤1 business day	Provide a resolution plan within 3 business days and agree completion with SACN.

"Response" means acknowledgement by an engineer who takes ownership, not an automated email. Record detection, notification, response and restoration timestamps. OEM dispatch times must be disclosed separately; an on-site response promise is not a guaranteed repair time. Include minimum next-business-day on-site OEM support for 36 months, with faster support where necessary for the contracted RTO.

15. REPORTING

Submit a monthly report by the fifth business day of the following month. Include availability, backup success and missed RPOs, restore-test outcomes, incident/SLA performance, usable capacity and growth, security/patch status, off-site-copy status, warranty dates and an action register with owners and due dates. Hold a quarterly service review.

Each report must also record approved expenditure, consumption-based charges, committed costs, remaining contract budget and anticipated renewals or capacity changes. Maintain an action register with owners and due dates and an auditable record of expenditure against approved amounts.

16. KEY PERFORMANCE INDICATORS

Performance area	Measure and evidence
Backup protection	Scheduled jobs complete within the agreed window and RPO; failures and stale recovery points are investigated and recorded.
Recovery readiness	Monthly sample restores, quarterly priority-data exercises and annual end-to-end recovery, including off-site recovery; results measured against Section 7.3.
Storage performance	Acceptance throughput of at least 500 MB/s read and 300 MB/s write under the conditions in Annexure A; ongoing capacity and health trends reported.
Support	Engineer response and action times meet Section 14.2; escalations and restoration timestamps are evidenced.
Security and maintenance	Approved patch actions, key recovery, protected-copy controls, access reviews and log retention are evidenced.
Delivery and financial control	Approved deliverables, training, monthly reports and change records completed; no unauthorised expenditure.

The provider must submit a test plan for SACN approval before migration. Execute tests using non-destructive simulations or controlled test data. SACN must witness the key recovery and access-control tests. Every mandatory requirement requires evidence; an installation checklist alone does not constitute acceptance.

Formal commissioning and acceptance tests are listed in Annexure A. Operational performance must be reviewed monthly and discussed at quarterly service reviews.

17. REQUIRED EXPERIENCE AND CAPACITY

Bidders must demonstrate successful delivery of enterprise storage and backup solutions of comparable scope and provide at least two completed deployments with contactable references.

- Experience with storage configuration, protected backup repositories, capacity planning and tested recovery.
- Ability to migrate file data and permissions and integrate with an existing directory service.
- Access to authorised supply channels and accountable hardware and software support.
- Capacity to provide the response coverage, on-site attendance, documentation and training required by this RFP.

Provide relevant certifications or demonstrably equivalent expertise. No particular manufacturer accreditation is compulsory unless justified by the support conditions of the offered product.

18. PROPOSED TEAM

Identify the personnel assigned to the project, their responsibilities, availability and escalation arrangements. Include CVs and relevant qualifications or equivalent experience for the functions below. Clearly nominate the lead storage and backup engineer and submit the certified qualification copies required for scoring under Section 20.3.

- Project or service-delivery lead.
- Storage and backup engineer.
- Network and security engineer.
- Migration and directory-integration specialist.
- Monitoring and support lead.

One person may fulfil more than one role where the bidder demonstrates sufficient competence and availability. Changes to key personnel during delivery require SACN's approval.

19. PROPOSAL REQUIREMENTS

19.1 Technical proposal

- Company profile, understanding of SACN's requirements and at least two signed client reference letters meeting Section 20.4.
- Executive proposal, solution diagram, deployment locations and a detailed bill of materials with exact makes/models, quantities, support terms and supplier accountability.
- Signed compliance matrix covering every requirement, with offered values, evidence and deviations. Include manufacturer datasheets and independent or reproducible performance evidence.
- Capacity and retention calculations using the common tender workload schedule; power/runtime calculations; recovery method; all network, identity and licensing dependencies.
- Implementation programme, migration/rollback plan, risk register, acceptance test plan, support SLA and escalation structure.
- Proposed team and CVs, support entitlements, data-processing arrangements, subcontractors and a complete statement of assumptions and deviations.

19.2 Financial proposal

- Commercial schedule with all once-off, recurring, consumption and optional costs; warranty evidence; data-processing approach; proposed subcontractors and exceptions.

Complete Section 12 and disclose the total proposed contract value, applicable VAT, payment milestones, quotation validity, unit rates, third-party costs, renewal estimates and separately priced options. Clearly identify every exclusion.

19.3 Compliance Documents

Bidders must submit the following documents together with their proposals:

- CIPC Registration Documents: Valid company registration documents confirming that the bidder is legally registered.
- Tax Compliance: A valid SARS Tax Compliance Status (TCS) PIN to enable verification of the bidder's tax compliance status.
- B-BBEE Certificate or Sworn Affidavit: A valid B-BBEE certificate issued by an accredited verification agency or a sworn affidavit confirming the bidder's B-BBEE status, as applicable.
- Joint Venture or Consortium Agreement (where applicable): Bidders submitting a proposal as a joint venture or consortium must provide a signed joint venture or consortium agreement clearly outlining the roles and responsibilities of each party, the lead partner, and the allocation of responsibilities for delivering the required services.

20. EVALUATION AND SELECTION CRITERIA

20.1 Technical evaluation

Only bids that meet the minimum functionality threshold of 75 points out of 100 (75%) will proceed to price evaluation. SACN reserves the right not to appoint the bidder who has quoted the lowest price.

Administrative eligibility and mandatory technical compliance will be checked against the published procurement requirements. Functionality scoring does not waive the mandatory storage, security, backup or recovery requirements of this RFP. SACN must publish the applicable price and preference rules in the final procurement pack.

Evaluation criterion	Weight / maximum points
Capacity and experience of the lead storage and backup engineer	20%
Qualifications of the lead storage and backup engineer	20%
Contactable client references	20%
Methodology and approach	40%
Total	100%
Minimum threshold to proceed to price evaluation	75%

20.2 Capacity and experience of the lead engineer

The bidder must provide an organogram and a detailed CV for the lead storage and backup engineer assigned to SACN. The CV must show dated experience in comparable enterprise storage, backup, migration and recovery assignments. If the relevant years cannot be established from the CV, zero points will be allocated. Count completed years without double-counting overlapping assignments.

Relevant experience	Points
Less than 1 year or no verifiable evidence	0
1 year	2
2 years	5
3 years	8
4 years	10
5 years	13
6 years	16
7 years and above	20

20.3 Qualifications of the lead engineer

The bidder must submit certified copies of the lead storage and backup engineer's relevant qualifications in information technology, computer science, information systems or a related technical discipline. Zero points will be allocated for qualifications not supported by certified copies. Score only the highest applicable qualification; points are not cumulative.

Highest relevant qualification evidenced	Points
No qualifying certified evidence	0
Certificate	5
Diploma	10
Degree or postgraduate qualification below a master's degree	15
Master's degree or higher	20

Product certifications and equivalent technical expertise may support the capability assessment, but do not replace the certified qualification evidence required for this criterion. No particular manufacturer's accreditation is prescribed.

20.4 Contactable client references

The bidder must submit a minimum of two reference letters for comparable completed enterprise storage and/or backup and recovery assignments. Each letter must describe the relevant work, name the client organisation and contact person, provide contact details, and be signed on the client's letterhead. SACN may contact the clients to verify the work. Count qualifying letters only; duplicate letters for the same assignment count once.

Qualifying reference letters	Points
No qualifying reference letters	0
1 letter	5
2 letters	10
3 letters	15
4 letters	20

A minimum of two qualifying reference letters is required for submission. The scoring band for one to two letters does not waive this requirement. Missing mandatory evidence is dealt with under the published eligibility requirements.

20.5 Methodology and approach

The bidder must submit a detailed methodology and project plan showing how it will supply, install, configure, migrate, commission and support the storage and backup solution while maintaining SACN's operations. The plan must identify tasks, delivery milestones, turnaround times, dependencies, resources and reporting responsibilities.

Assessment component	Maximum points
Methodology with clear activities and turnaround times	30
Distribution of resources and reporting structure	10
Total for methodology and approach	40

Methodology with clear activities and turnaround times

The assessment covers the completeness, feasibility and evidence supporting the following activities:

- Assessment and design: validate workloads and site dependencies; provide the architecture, bill of materials, capacity and retention model for the 48 TB raw primary and 64 TB raw backup configurations, with 64 GB ECC memory per system.
- Installation and integration: address RAID protection, 10GbE connectivity, UPS protection, directory permissions, encryption, separate administration and platform hardening.
- Migration and continuity: provide the phased migration plan, approved downtime, integrity and permission checks, rollback steps and arrangements to keep users working.
- Backup and recovery: configure independent and protected off-site copies, immutable or offline retention, monitoring and escalation; demonstrate the required RPO/RTO through Annexure A acceptance tests.
- Handover and support: provide training, operating and recovery procedures, a delivery timetable and 24 months of monitoring and operational support, with the Section 14 response and resolution targets addressed.

Distribution of resources and reporting structure

Provide named personnel and role allocation, availability for each implementation phase, support cover, escalation contacts, subcontractor responsibilities and reporting lines to SACN. Explain how resources will cover migration, recovery testing, handover and the ongoing support period.

Scoring basis

Score each component within its stated range (0–30 and 0–10). Award zero where evidence is absent or irrelevant; partial points where the approach is incomplete, generic or weakly evidenced; and full points only for a complete, feasible and assignment-specific response covering all stated elements. Evaluators must record evidence and reasons for the points awarded. The two component scores are added, not weighted again.

21. CONTRACT PERIOD

The contract comprises once-off design, supply, installation, migration and commissioning, followed by 24 months of monitoring and operational support from formal acceptance. The commencement date will be confirmed in the appointment documentation. Hardware warranty and support must continue for at least 36 months from acceptance.

Include the storage operating system, backup software, agents, management features, encryption, replication, immutable retention and all access licences needed for the offered configuration. State licence metrics, capacity/workload limits and renewal dates. All subscriptions must cover the full 24-month service period from acceptance; hardware support must cover at least 36 months.

Any extension is subject to SACN's procurement requirements, performance, funding and written approval. Renewal prices and service behaviour after subscription expiry must be disclosed before award.

22. ASSUMPTIONS AND EXCLUSIONS

The base scope covers organisational file data and the supplied storage/backup configuration. Application-aware database, virtual machine, email, Microsoft 365 and endpoint backups are excluded unless expressly added to the workload schedule. Major building electrical work, a new cabinet and WAN upgrades must be separately identified and priced where required. No unpriced dependency may be assumed to be available.

Two standalone servers provide separation and recovery capability; they do not constitute automatic production failover. A clustered high-availability design may be priced as a separate enhancement.

The capacities and service levels in this document are proposed requirements, not measured characteristics of SACN's current environment. SACN must confirm the procurement particulars and workload schedule before issue.

SACN must confirm installation and alternate recovery locations, rack and power readiness, existing switches, directory versions, client compatibility, WAN bandwidth, source data and required access before issue. All bidders must use the same baseline; unconfirmed reuse must have a priced supply option.

Travel and after-hours assumptions must be disclosed and included where necessary to meet contracted obligations. Optional clustering, additional power resilience, extended retention and additional capacity require separate pricing and approval. No additional charge may be raised for an item represented as included in the accepted offer.

23. INTELLECTUAL PROPERTY AND CONFIDENTIALITY

SACN retains ownership and control of its data, configurations, reports and recovery keys. The service provider may process data only for authorised delivery and support activities. Conclude a written confidentiality and data-processing agreement addressing security measures, personnel access, subcontractors, incident escalation, return of data and secure deletion. These controls support the security and operator requirements in POPIA sections 19-22. [3]

The provider must notify SACN immediately where there are reasonable grounds to believe personal information was accessed or acquired by an unauthorised person, and preserve evidence. SACN will direct its statutory notifications and incident response. The service provider must not publish incident details or move data to another location without authority. [3]

Register assets and entitlements in SACN's name where supported. Disclose perpetual versus subscription rights and the ability to restore after expiry. Provide export in commonly usable formats, administrative documentation and a 30-day planned exit handover within the contract price. No exclusive dependence on the supplier for access to SACN's own data is acceptable.

Project-specific documentation, configurations and reports developed for SACN must be handed over in editable or commonly usable formats. Pre-existing supplier intellectual property and third-party software remain subject to disclosed licence terms that permit SACN to operate and recover its data.

24. VALUE FOR MONEY

Bidders must demonstrate value over the complete implementation and support period. Evaluate usable capacity, resilience, recovery performance, licence completeness, operational effort and renewal costs together with the purchase price.

- Reuse existing SACN infrastructure only where its capability and support status have been verified.
- Provide a supported expansion path and price upgrades separately so capacity can be added when justified.
- Avoid proprietary dependencies that prevent SACN from restoring or exporting its data.
- Include practical administrator training, complete handover and measurable recovery tests.
- Separate optional enhancements from the base offer and obtain approval before incurring additional costs.

25. ANNEXURES

- Annexure A - Testing and acceptance schedule.

The annexures form part of this RFP.

ANNEXURE A TESTING AND ACCEPTANCE SCHEDULE

Test	Minimum pass criterion / evidence
Inventory and sizing	Verify 48 TB raw primary (6 × 8 TB) and 64 TB raw backup (4 × 16 TB), each in RAID 6 with approximately 32 TB before overheads; 64 GB RAM per server. Record formatted capacity and confirm the approved retention/headroom model.
Security and access	Successful directory access for authorised test users; denial for unauthorised users; encryption, administrative MFA, log export and key recovery demonstrated; no unresolved critical security defects.
Resilience and power	Demonstrate controlled loss of a network path and power supply without data loss. Validate dual-parity configuration and rebuild procedures. Test UPS runtime, alerts and graceful shutdown/restart under agreed safe conditions.
File-service performance	At least 500 MB/s sequential read and 300 MB/s sequential write aggregate on a verified 10GbE path, with encryption and protection enabled. Use ≥500 GB non-compressible test data and sustained runs ≥15 minutes; bypass/exhaust cache and document clients and method.
Migration integrity	Approved source/destination manifests reconcile. Critical files and the agreed sample pass hash checks; permissions and usability verified. All unexplained data-loss exceptions resolved before acceptance.
Backup and immutability	Successful full and incremental cycles; alerts tested; future expiry schedule verified. Attempt deletion of a retained test point using a production admin account: deletion must be prevented. Validate offline custody where used instead.
Recovery	Restore up to 10 GB within 1 hour and the agreed priority dataset up to 1 TB within 8 hours, including permissions and service access. Demonstrate recovery without the primary server and test off-site recovery against the 72-hour target.
Full recovery model	Demonstrate the full in-scope dataset recovery within 48 hours, or agree a representative measured test plus a conservative whole-dataset projection before award. Record exactly what was tested and what was modelled.
Stabilisation and handover	10 consecutive business days with scheduled backups completing within the agreed window/RPO, no unresolved P1/P2 defects, full handover pack delivered and training completed.

SACN must witness the principal recovery and access tests. Record the result, evidence reference, witness, date and corrective action for each test. Failed tests must be corrected and repeated before acceptance, subject to the acceptance provisions in Section 13.

26. SUBMISSION

Email all submissions to Mr Jabulani Sandleni at Jabulani@sacities.net by close of business on Tuesday, 28 October 2026 at 17:00 (5 pm).

Note that only proposals submitted to the email address specified in the RFP and received on or before the stipulated closing date and time will be considered. Proposals received after the closing date and time will not be considered.

All clarifications affecting scope, pricing or evaluation must be made available consistently to prospective bidders. The final procurement notice will govern submission arrangements.