

SOUTH AFRICAN REVENUE SERVICE

REQUEST FOR PROPOSAL

RFP 03/2026

**THE APPOINTMENT OF A SERVICE PROVIDER FOR THE PROVISION OF
SERVER SUPPORT SERVICES (TOWER S), FOR A PERIOD OF THREE (3)
YEARS, WITH AN OPTION TO EXTEND FOR TWO (2) YEARS.**

BUSINESS REQUIREMENTS SPECIFICATION

Table of Contents

1	USAGE OF TERMS IN THIS DOCUMENT	5
1.1	REFERENCES TO OTHER DOCUMENTS IN THE RFP PACK	5
1.2	GLOSSARY TABLE	5
1.3	MANDATORY AND DIRECTORY REQUIREMENTS.....	6
1.3.1	Mandatory Requirements (Summary)	7
2	BACKGROUND	8
3	COMPONENTS OF SCOPE.....	9
4	USE OF ALTERNATE TECHNOLOGIES OR PROCESSES DURING THE TERM	9
5	UNDERLYING PRINCIPLES TO THE SERVICES	9
5.1	ACCOUNTABILITY.....	10
5.2	NON-EXCLUSIVE.....	10
5.3	FLEXIBILITY.....	10
5.4	TECHNICAL TRANSFORMATION	11
5.5	COMPLIANCE.....	11
5.6	PERFORMANCE STANDARDS	11
5.7	SERVICE LEVELS AND SERVICE COVERAGE PERIODS.....	12
5.8	SPECIFICATION OF SERVICE COVERAGE PERIOD AND SERVICE LEVEL FOR A SERVER DEVICE	12
5.9	CHANGE OF SERVICE COVERAGE PERIOD AND SERVICE LEVEL	13
5.10	MEASUREMENT AND REPORTING SERVICE LEVELS.....	13
5.11	REQUEST TO EXPEDITE REPAIR OR SERVICE.....	13
5.12	OEM RELATIONSHIP	14
5.13	MANDATORY INFORMATION SECURITY REQUIREMENTS	15
6	SERVICE DEFINITIONS AND REQUIREMENTS.....	18
6.1	SERVICE MANAGEMENT	18
6.2	DEVICE-BASED SERVICES	20
6.3	SERVICE DESCRIPTIONS	21
6.4	GENERAL OBLIGATIONS APPLICABLE TO ALL DEVICE-BASED SERVICES.....	21
6.5	GENERAL HOUSEKEEPING ACTIVITIES	21
6.6	BREAK-FIX SERVICE DESCRIPTIONS	22
6.7	BREAK-FIX SERVICES REQUIRED FOR DEVICES UNDER WARRANTY.....	22
6.8	BREAK-FIX SERVICES REQUIRED FOR DEVICES NOT UNDER WARRANTY.....	23
6.9	BREAK-FIX SERVICES FOR SERVER DEVICES THAT REQUIRE ONLY THE FACILITATION OF REPAIR.....	23
	(EXCLUDE ACTUAL REPAIR ACTIVITIES)	23
6.10	BREAK-FIX SERVICES THAT QUALIFY FOR PERMANENT REPLACEMENT.....	24
6.11	WUS SERVICES	24
6.12	SUMMARY OF BREAK-FIX SERVICES AND RELATED PROCESS FLOWS	24
6.13	STANDARD CHARGEABLE SERVICES.....	25
6.14	MISCELLANEOUS SERVICES	26
6.15	SERVICE PROVIDER MANAGEMENT PERSONNEL.....	30
6.16	PROJECT SUPPORT	31
6.17	CONSULTING.....	31
6.18	TRAINING.....	31
6.19	ADMINISTRATION	31
7	RESEARCH AND DEVELOPMENT	32
8	TRANSITION PROCESS	32
8.1	TRANSITION PLAN.....	32
8.2	EXPERIENCED TRANSITION TEAM.....	33
9	TOWER S: SERVER SUPPORT SERVICES	33

9.1	SCOPE	33
9.2	FLEXIBLE SUPPORT SERVICES	35
9.2.1	Adaptive Service Delivery	35
9.2.2	Proactive Technology Support	35
9.2.3	Scalable Support Model	35
9.2.4	Agility in Service Implementation	35
9.2.5	Collaborative Approach	35
9.3	DELIVERY MODEL	36
9.4	TRANSITION	36
9.5	DEVICE-BASED SERVICES APPLICABLE TO TOWER S	37
9.6	SERVICE COVERAGE PERIODS AND SERVICE LEVELS APPLICABLE TO TOWER S	39
9.7	SERVICE PROVIDER TECHNICAL PERSONNEL	41
ATTACHMENT A: PROCESS FLOW DIAGRAMS		42
1.	IN-WARRANTY BREAK-FIX PROCESS (WUS NOT APPLICABLE)	43
DIAGRAM 1.1 BREAK FIX (IN WARRANTY)		44
2.	SERVICE-ONLY TIME AND MATERIAL PROCESS (WUS NOT APPLICABLE)	44
DIAGRAM 2.1 SERVICE ONLY TIME AND MATERIAL (OUT OF WARRANTY)		44
3.	SARS-PROVIDED WUS PROCESS	45
DIAGRAM 3.1 SARS PROVIDED WUS PROCESS		45
4.	INSTALLATION/REPLACE PROCESS	46
DIAGRAM 4.1 INSTALLATION/REPLACEMENT PROCESS		46
5.	MOVE PROCESS	47
DIAGRAM 5.1 MOVE PROCESS		47
6.	DECOMMISSION FOR DISPOSAL	48
DIAGRAM 6.1 DECOMMISSIONING FOR DISPOSAL		48
7.	DELIVERY ACCEPTANCE TEST	49
DIAGRAM 7.1 DELIVERY ACCEPTANCE TEST		49

RFP 03/2026**Business Requirements Specification**

This document forms part of the RFP 03/2026 pack. It sets out the business requirements that SARS has for Server Device Support Services. This document and its attachments must be read in conjunction with all other documents in the RFP Pack as they may contain further requirements that must be considered by the Bidder in compiling a Proposal. The Bidder is referred, in particular, but without limitation to the following documents in the RFP Pack:

- Main RFP Document;
- Server Device Support Services Agreement;
- Tower S Site Classifications;
- Tower S Server Devices, per SARS Site.

The Server Device Support Services Agreement sets out the provisions of the agreement under which SARS intends to contract with the successful Bidder(s). The Server Device Support Services Agreement contains the contractual provisions for Tower S. Provisions that are only applicable to Tower S are clearly marked in the Server Device Support Services Agreement. While the Bidder is required to respond to the Server Device Support Services Agreement, of particular relevance to this Business Requirements Specification are the following Schedules and Appendices which must be read in conjunction with this document:

- Schedule B (Service Management SOW),
- Schedule B-S (Server Support Services SOW
- Schedule C (Service Levels),
 - Appendices C-S-1 and C-S-2,

1 USAGE OF TERMS IN THIS DOCUMENT

1.1 References to other Documents in the RFP Pack

Underlined and italicized names are references to (or short names of) other documents in the RFP Pack. The Bidder must refer to paragraph 4 of the Main RFP Document for the table of documents and their short names.

1.2 Glossary Table

The capitalized terms in this document appearing in the glossary table below will have their corresponding meanings.

Term	Meaning
API	Application Programming Interface
CSIRT	Computer Security Incident Response Team
CMDB	Configuration Management Database
Device-based Services	Services relevant in the context of a device, including break-fix services in the event of a device not functioning according to specification and services provided on request, such as the install, move, add, change or decommission of a device.
Expedited Service Request	See the definition in paragraph 5.12
HBA	Host Bus Adaptor
In-warranty	Referring to the status of a device that is under manufacturer warranty.
KVM	Keyboard, Video and Mouse
OEM	The original equipment manufacturer.
Out-of-support	Referring to the status of a device that is no longer supported by the OEM. I.e. the OEM no longer manufactures spare parts; issues fixes for; or otherwise provide any support for, the device.
Out-of-warranty	Refers to the status of a device that is not under manufacturer warranty.
SARS PPS&G	SARS Policies, Procedures, Standards and Guidelines
SARS Service Management System	The BMC Remedy system used for the management of SARS' service management processes.
SD Card	Secure Digital Card
SDLC	System Development Lifecycle
Seat	Open-plan office space on a SARS site containing a desk, chair, and network connection point.

Term	Meaning
Server	Enterprise computing platforms. The scope of this RFP includes servers based on the Intel processor family.
Service Coverage Period	See the definition in paragraph 5.
Service Level	See the definition in paragraph 5.
Service-only	A type of service in which the Service Provider is required to <u>facilitate</u> the restoration of services and in which a third party may perform the actual repair of the device and for which SARS is responsible for the costs of such a third party. See paragraph 6.9.
Services	The services to be delivered by the Service Provider as set out in clause 4 of the <u>Server Device Support Services Agreement</u> .
SFP	Small Form Factor Pluggable.
SIEM	Security Information and Event Management
Site Classification	See definition in paragraph 5.
SOW	Statement of Work
SOC	Security Operation Centre
SOAR	Security Orchestration, Automation and Response
SP	Service Provider.
Standard Chargeable Services	Defined packages of work that are performed by the Service Provider on request by SARS at a fixed rate per request. For example: the installation of a computing device. The Standard Chargeable Services are set out in paragraph 6.13.
Swap-out	Means the activity of permanently replacing a non-functioning device with a functioning device. See paragraph 6.10.
UTR or Uneconomical to Repair	This term is applicable to the handling of certain repairs to out-of-warranty devices for which the Service Provider is obligated to repair a monthly charge. See paragraph 6.8.
WFH	Work from Home.
WUS or Whole Unit Spare	An entire functioning device to replace a non-functioning device temporarily, while the non-functioning device is being repaired or replaced. The device must deliver at least the same functionality as the non-functioning device.

1.3 Mandatory and Directory Requirements

Bidders are advised to read the business requirements as set out in this document with care. Where SARS has specified a mandatory requirement, (i.e., where the business requirement, by the context; presence of verbs such as 'must'; 'will'; 'shall' etc.; or explicit instruction indicating that it is mandatory), the Bidder must build and price its solution accordingly.

1.3.1 Mandatory Requirements (Summary)

Compliance to RFP Pack: The Bidder **must** comply with, and respond to, all requirements contained in this Business Requirements Specification (BRS) and all other documents in the RFP Pack.

- **Single accountable Service Provider:** The Bidder **must** be able to assume end-to-end accountability for Tower S services, including accountability for all subcontractors, OEM partners, couriers and third-party repair providers.
- **Subcontracting limitation:** The Bidder **must not** subcontract more than 40% (forty percent) of the business by revenue and **must** contractually bind any approved subcontractors to obligations no less stringent than those imposed on the Service Provider.
- **OEM back-to-back agreements and certification:** The Bidder **must** have (by Commencement Date) back-to-back support agreements in place with applicable OEMs (or their official representatives) and relevant OEM partner certifications for the equipment in scope Dell server equipment).
- **Service Levels and reporting:** The Bidder **must** meet or exceed all Service Level targets and **must** measure and report Service Levels monthly in accordance with Schedule C of the Server Device Support Services Agreement, using data from the SARS Service Management System.
- **Service coverage:** The Bidder **must** provide services in accordance with the Service Coverage Periods and Service Levels assigned to SARS sites (including Metro, Town and Rural site classifications) and must support devices at the site where they are physically located, subject to the rules defined in this BRS.
- **Information security compliance:** The Bidder **must** comply with all SARS Policies, Procedures, Standards and Guidelines (PPS&G), including information security, cyber security, access control and data protection requirements, as amended from time to time.
- **Security standard alignment:** The Bidder **must** align to ISO/IEC 27001 (or equivalent internationally recognised information security standard) for the full duration of the Agreement and provide evidence of compliance upon request by SARS.
- **Personnel vetting and confidentiality:** All Bidder personnel requiring access to SARS sites, systems or devices **must** undergo SARS-approved vetting (including Oath of Secrecy screening) prior to access being granted, and confidentiality obligations **must** remain in effect beyond termination.
- **Access control:** The Bidder **must** ensure least-privilege access, prohibit credential sharing, and comply with SARS requirements for time-bound, approved and auditable privileged access, including MFA where technically feasible.
- **Incident handling and breach notification:** The Bidder **must** notify SARS without undue delay of any actual or suspected security incident, data breach, or loss/theft/compromise of a SARS asset and cooperate fully with SARS SOC/CSIRT and investigations.
- **IT Service Management capability:** The Bidder **must** have a mature IT Service Management capability and **must** hold ISO 20000 certification or provide a formal IT Service Management maturity assessment evidencing an overall maturity score of 4 (quantitatively managed) or higher.
- **Tooling and interface:** The Bidder **must** provide a 24x7 external web interface for incident/problem reporting and status updates and **must** be

able to receive, route and update tickets on the SARS Service Management System using SARS-provided licenses (with any additional licenses at the Service Provider's cost).

- **Break-fix delivery:** The Bidder **must** provide the required Break-fix services (in-warranty, out-of-warranty/time and materials, service-only facilitation, WUS and swap-out where applicable) and restore devices to last working configuration as defined in this BRS and the Agreement.
- **Spare parts authenticity and supply chain controls:** The Bidder **must** implement controls to verify authenticity and integrity of parts, firmware, and whole unit spares (WUS), and ensure only OEM-approved, digitally signed firmware is installed following SARS change management requirements.
- **Physical security and chain of custody:** The Bidder **must** ensure secure handling, storage and transport of SARS devices and maintain a documented chain of custody for all device movements.
- **Data protection and sanitisation:** The Bidder **must** comply with POPIA and SARS confidentiality obligations and **must** perform certified data sanitisation for devices subject to swap-out, WUS replacement, and decommissioning, in accordance with SARS PPS&G.
- **Transition:** The Bidder **must** provide a transition plan and execute transition activities to achieve a successful transition and minimise disruptions, within the maximum transition period specified in this BRS.
- **Pricing submission:** The Bidder **must** provide pricing as required for the combinations of Site Classification, Service Coverage Period and Service Level, as well as fixed rates for Expedited Service Requests, and pricing for Standard Chargeable Services per site classification, in the format required in the RFP Pack.

Directory requirements (i.e., where the business requirement, by the context; presence of verbs such as 'may', 'should', 'can' etc.; or explicit instruction indicating that they are directory) are requirements that SARS does not regard as mandatory.

2 BACKGROUND

SARS currently makes use of server equipment from original equipment manufacturer (OEM), Dell. This Business Requirements Specification (BRS) forms part of the RFP pack and sets out the requirements that bidders must address in their proposals for the provision of Server Device Support Services.

To achieve SARS's Vision of a smart, modern SARS with unquestionable integrity that is trusted and admired is of paramount importance. Pivotal to the delivery of SARS' vision are our digital platforms and technology infrastructure. To foster Strategic Objective 9, of building public trust and confidence, our technology assets must demonstrate the highest levels of robustness and security. It is indeed for these reasons, inter alia, that SARS's measure it on a planned 99% uptime and zero security breaches from known risks. In support of this, the mandate is executed, among others, through partnering with third-party suppliers to provide services and products to enable achievement of organizational objectives.

This tender for the Tower S device support services aligned with several of SARS's Strategic Objectives, including:

- Objective 1: Clarity and certainty for taxpayers and traders of their obligations;
- Objective 2: Make it easy for taxpayers and traders to comply with their obligations;

- Objective 6: Modernise our systems to provide Digital and Streamlined services; and zero security breaches from known risks.
- Objective 5: Increase and expand the use of Data within a comprehensive knowledge management framework to ensure integrity, drive insight and improve outcomes.

The primary objective of this RFP is to ensure the continuity and cost-effectiveness of SARS's Server device support services. SARS's objectives in issuing this RFP do not include a transformation of the technologies or services related to the support of SARS's Server devices. However, during the anticipated Term of the Server Device Support Services Agreement, developments in, Server Device technologies, including technologies to manage such environments, require that SARS maintains a flexible approach in contracting Service Provider(s) to ensure that it can take advantage of these developments and ensure the support methods and processes keep abreast of developments in this field.

The landscape of server devices is constantly evolving and as SARS maintains its efforts to modernize its systems, a changing mix of devices, brands and models are anticipated to be introduced during the Term of the Server Device Support Services Agreement. It will, therefore, be expected of the Service Provider(s) to support a wide and evolving range of server devices as and when SARS may introduce them into the SARS configuration, although the award of a contract does not confer the right of exclusivity to provide support services for new devices.

3 COMPONENTS OF SCOPE

SARS scope of the RFP Towers S

4 USE OF ALTERNATE TECHNOLOGIES OR PROCESSES DURING THE TERM

In defining the scope of Tower S, reference is made to technologies and/or specific processes currently deployed within the SARS environment. Where a technology or process has been specified in this Business Requirements Specification the Bidder's Proposal must be designed to comply with the specific technology and/or process.

During the Term of any agreement arising from the award of this RFP, the use of alternative technologies and/or processes may be proposed by the Service Provider and/or requested by SARS and their implementation will not be considered out of scope of the award, provided that they effectively substitute, or supplement technologies/processes contained in the Service Provider's original Proposal. No alternative technologies/processes may be implemented during the Term without SARS' approval.

5 UNDERLYING PRINCIPLES TO THE SERVICES

The principles detailed in this paragraph apply to the Services to be delivered in Tower S.

5.1 Accountability

SARS requires a single, accountable Service Provider for the Services to be delivered in Tower S. The Service Provider must engage all subcontractors on a formal contractual basis and must ensure adherence to the conditions placed on subcontractors as required by SARS. To ensure sufficient control is retained by the Service Provider, the Service Provider is limited to subcontracting no more than 40% (forty percent) of the business, by revenue. For further details on the conditions attached to the Service Provider's use of subcontractors, see paragraph 9 of the Main RFP Document.

The Service Provider must supply all elements of the Services to SARS in the Service Provider's name. The Bidder must not propose a solution in any part of its Proposal that is contingent on SARS granting the Bidder an agency for it to procure elements of the solution from a third party in SARS's name.

5.2 Non-exclusive

SARS intends to contract for the different areas of scope with the Service Provider on the basis that certain of the Services (or categories of such equipment or equipment located in certain locations) may be excluded from the scope.

SARS will retain the right to source any part of the scope of Services from other Service Providers during the Term or to provide such part of the scope of Services itself.

5.3 Flexibility

During the Term of the agreement SARS anticipates that it will change the landscape of its infrastructure and configuration and the requirements for the support thereof. SARS, therefore, retains the right to adapt the scope of equipment and processes to its changing requirements including the right to:

- Include new categories and/or exclude current categories of equipment, with regards to new categories the Service Provider will be given 90 (ninety) days' notice to enable the new category;
- Include new manufacturers/brands models and/or exclude current manufacturers/brands/models of equipment;
- Increase or reduce the quantities of equipment under support;
- Introduce equipment at new sites into the scope of support or exclude equipment at existing sites from the scope of support; and
- Include or exclude existing or new sites from the scope of services.

Therefore, a Bidder must be prepared to contract to provide support services on a flexible basis to accommodate SARS's changing needs and requirements for support of changing technologies.

5.4 Technical Transformation

SARS has no specific or immediate requirement to undertake a major technical transformation in terms of the technology or processes as part of the Services. If SARS undertakes a transformation of technology or process within the scope of a Tower during the Term, the Service Provider appointed may be engaged, on a project basis, to provide services supporting the transformation. For clarity, while a yearly percentage of refresh of equipment is undertaken by SARS on a continuous basis, this is not considered a technical transformation and SARS may reduce the number of devices to be supported.

5.5 Compliance

The Service Provider is required to execute the processes, procedures, schedules and work practices developed in accordance with the Server Device Support Services Agreement. Throughout the Term of the agreement, the Service Provider will be required to improve and modify these processes, procedures, schedules and work practices as required by SARS.

The Bidder must note the obligation to adhere to SARS PPS&G in the Server Device Support Services Agreement.

5.6 Performance Standards

It is of critical importance to SARS that the Service Provider provides the Services to meet or exceed the Service Levels specified in Schedule C of the Device Support Services Agreement and its Appendices. The Service Provider will be required to measure, monitor and report upon the delivery of the Services against the Service Levels. The Service Provider must draw performance-related information from the SARS Service Management System to construct and produce the required monthly reports on Service Level achievements. The information to be presented in the report and the format of the report will initially be agreed upon between the Service Provider and SARS during Transition and will be continuously improved during the Term. The Service Level requirements are set out at a high level with explanatory notes in this document but must be read together with Schedule C of the Server Device Support Services Agreement.

The Bidder's attention is drawn to the Service Level Targets and the provisions of Schedule C of the Server Device Support Services Agreement regarding Service Level Credits.

SARS will assign a Site Classification (Metro, Town or Rural) to each SARS Site. The Bidder must consult SARS Site Classifications to obtain the Site Classification that will be associated with each SARS site at the Effective Date. The Site Classification will be one of the factors determining the price of support for devices at a SARS Site.

5.7 Service Levels and Service Coverage Periods

The definition of the performance standards applicable to a device category is specified with respect to two dimensions: Service Coverage Period and Service Level.

“**Service Coverage Period**” relates to the hours of service applicable to a device that will be one of Basic, Standard, Extended or Premium.

“**Service Level**” relates to the time within which the Service Provider must respond and repair the device. The Service Level is specified by a Service Level Class (Bronze, Silver, Gold) which describes the repair time applicable to a server device (and may, in certain cases, be specified in terms of response time).

SARS requires the Bidder to quote a monthly rate for every applicable server device-based service for every combination of Site Classification (Metro, Town or Rural); Service Coverage Period Basic, Standard, Extended and Premium) and Service Level (Bronze, Silver or Gold) for every device type.

The definitions of Bronze, Silver or Gold within Tower S and the definitions of Basic, Standard, Extended and Premium within Tower S are set out under the *service descriptions paragraph 6.3* of this document, respectively.

5.8 Specification of Service Coverage Period and Service Level for a Server Device

In each Tower, each SARS Site has been assigned a Service Level and Service Coverage Period that applies to all server devices in the Tower that are registered to that SARS Site. At the Commencement Date, the Service Level and Service Coverage Period assigned to a site will be as specified in SARS Site Classifications per Tower S. SARS may change the Service Level and Service Coverage Period assigned to a SARS Site during the Term with 60 (sixty) days’ notice.

If support is required for a server device which has been moved from the site at which it is registered, then the Service Provider must still provide support for the server device at the SARS site to which it has been moved, subject to the following:

- The shorter of the Service Coverage Periods between the SARS site to which the device is registered and the SARS site to which the device has been moved will apply.
- The least stringent of the Service Levels between the SARS site at which the device is registered and the SARS site to which the device has been moved will apply.
- For example:

A server registered at Beit Bridge has a Service Coverage Period of “Standard” and a Service Level of “Silver”. The server is moved to Lehae la SARS in Brooklyn, which has a Service Coverage Period of “Premium” and a Service Level of “Bronze”. The Service Coverage Period and the Service Level applied to the device will be “Standard” and “Bronze”, respectively, although SARS is being charged for a “Standard” and “Silver” service for the device. This example is set out in the table below.

Table 1: Service Coverage Period of Standard and a Service Level of Silver

Service Coverage Period	Site at which the Device is registered	Site where the Device is physically	Applicable Service Level
Service Coverage Period	Standard	Premium	Standard
Service Level Class	Silver	Bronze	Bronze

(Note that the values for Service Coverage Period and Service Levels in the example above are for illustrative purposes only and the Bidder must consult SARS Site Classifications as per Tower S for the actual Service Coverage Periods and Service Levels that are specified for each SARS site).

5.9 Change of Service Coverage Period and Service Level

The Bidder must provide rates for all combinations of Site Classification, Service Coverage Period and Service Level requested for all categories of devices. SARS may, during the Term, with 60 (sixty) days' notice, change the Service Level and/or Service Coverage Period that applies to a SARS site. The rates associated with the new Service Level and Service Coverage Period must be charged from the day the new Service Level and Service Coverage Period come into effect.

5.10 Measurement and Reporting Service Levels

The Service Provider must produce monthly Service Level reports in accordance with Schedule C of the Server Support Services Agreement. In this regard, the Service Provider must produce the reports using data from the SARS Service Management System. The method of obtaining the data from SARS Service Management System must be determined and processes defined as part of the Transition project.

5.11 Request to Expedite Repair or Service

Regardless of the Service Coverage Period associated with a device, SARS may request that the Service Provider attends to the repair or service of a specific server device outside the Service Coverage Period attached to the device. This service request is known as an **"Expedited Service Request"**. The Bidder is required to provide a fixed rate, which is chargeable with every Expedited Service Request that SARS makes.

This fixed rate is only related to the elements of costs of expediting the services and must not include any costs related to the repair or service that already forms part of another rate/charge associated with the repair or service.

An Expedited Service Request will be initiated by a request from an approved member of SARS personnel to the Service Provider. During Transition, SARS will confirm the names of the SARS personnel that may approve an Expedited Service Request. On receipt of a request from SARS, the Service Provider must offer SARS a committed time of arrival at the site and/or a committed time to repair. SARS may accept or reject such offer provided by the Service Provider. If SARS accepts the Expedited Service Request offer, the Service Provider will provide the expedited services at the associated Expedited Service Request rate. If the Service Provider does not meet the committed time of arrival on site and/or the committed time to repair after acceptance by SARS of the offer, no part of the Expedited Service Request rate is payable by SARS. The acceptance or rejection of the Service Provider's offer by SARS will in no way relax the base Service Level already applicable to the device(s).

The Service Provider must provide a monthly report detailing the Expedited Service Requests attended to during the preceding month. The Service Provider must analyse the Expedited Service Requests and include recommendations for ways to reduce the number of Expedited Service Requests in the monthly report.

5.12 OEM Relationship

The Service Provider must have a back-to-back agreement in place with the applicable OEMs (or their official representatives) and OEM partner certification in support of the equipment for which the Service Provider is contracted to provide services to SARS. SARS's requirement is for the Service Provider to have the back-to-back agreements in place and partner certifications with the applicable OEMs by the Commencement Date. On OEM renewals, if the Service Provider fails to meet the obligations on an annual basis, then the penalty under Common Service (Schedule C (*Service Levels*) of the *Server Support Services Agreement* will apply.

The Service Provider must ensure that the back-to-back agreement for all services remains effective throughout the Term of the Server Device Support Services Agreement.

During the Term of the agreement, SARS may elect to change the equipment/brands currently used within SARS or introduce new equipment from a new manufacturer. The Service Provider must be prepared to enter into new/additional back-to-back agreements and partner certifications within 90 days with OEMs (or their official representatives) to accommodate SARS's requirement for support for the newly introduced equipment/brands.

5.13 Mandatory Information Security Requirements

a. Information Security Governance & Compliance

- The Service Provider shall comply with all SARS Policies, Procedures, Standards and Guidelines (PPS&G), including but not limited to information security, cyber security, data protection, and access control requirements, as amended from time to time.
- The Service Provider shall align to ISO/IEC 27001 or an equivalent internationally recognised standard for the full duration of the Agreement.
- Upon request by SARS, the Service Provider shall provide evidence of certification, independent assurance reports, or formal attestations demonstrating compliance with its security obligations.
- Failure to comply with security requirements shall constitute a **material breach** of the Agreement.

b. Third Party, Subcontractor and Supply Chain Security

- The Service Provider shall remain fully accountable for the security posture, actions, and omissions of all subcontractors, OEM partners, couriers, and third-party repair providers.
- The Service Provider shall not subcontract any service involving access to SARS systems, data, or devices without prior written approval from SARS.
- All subcontractors and third parties shall be contractually bound to security obligations no less stringent than those imposed on the Service Provider.
- The Service Provider shall implement supply chain risk management controls, including verification of the authenticity and integrity of:
 - Hardware components
 - Firmware
 - Whole Unit Spares (WUS)
 - Replacement parts

c. Personnel Security, Vetting and Confidentiality

- All Service Provider personnel accessing SARS sites, systems, or devices shall undergo SARS-approved vetting, including Oath of Secrecy screening, prior to access being granted.
- The Service Provider shall ensure ongoing confidentiality obligations for all personnel, including after termination of employment or contract.
- SARS reserves the right to deny or revoke access for any Service Provider personnel at its sole discretion without prejudice.
- The service provider shall ensure timely notification of personnel termination or any changes in support roles during term of contract.

d. Access Control & Privileged Access Management

- SARS shall implement strict role-based access control (RBAC) ensuring personnel have access only to the minimum privileges required to perform their duties.

- All privileged access to SARS systems shall be time-bound, auditable, and approved by SARS.
- The Service Provider shall not share credentials under any circumstances.
- Multi-factor authentication (MFA) shall be mandatory for all access to SARS systems where technically feasible.
- SARS will implement session logging, monitoring, or recording for privileged activities.

e. System Integration & Interface Security

- Any system integration between the Service Provider and SARS environments shall be subject to SARS security architecture approval prior to implementation.
- All interfaces, APIs, and integrations shall:
 - Use strong authentication mechanisms
 - Encrypt data in transit
 - Be restricted to approved network zones
 - Be documented and approved
- The Service Provider shall not expose SARS systems to additional interfaces or network connections without explicit written approval.
- SARS reserves the right to suspend or terminate integrations deemed to pose a security risk.

f. Data Protection, Privacy & POPIA Compliance

- The Service Provider shall protect all SARS data, including taxpayer and confidential information, in accordance with:
 - POPIA
 - SARS confidentiality obligations
 - Applicable legislation and regulations
- The Service Provider shall not copy, store, process, or transmit SARS data outside of approved environments.
- Data shall not be removed from SARS devices unless explicitly authorised in writing.

g. Data Sanitisation & Device Lifecycle Security

- All devices subject to:
 - Swap out
 - WUS replacement
 - Decommissioning (re use or disposal)
- shall undergo certified data sanitisation aligned to recognised standards (e.g. NIST aligned wiping).
- The Service Provider shall provide evidence of data destruction or sanitisation upon request as per SARS PPS&G.
- WUS devices shall be data clean, hardened, and approved before installation in the SARS environment.

h. Firmware, BIOS and Platform Security

- The Service Provider shall ensure only OEM approved, digitally signed firmware is installed on SARS devices.

- Firmware updates shall follow SARS change management procedures and must not introduce downgrade or integrity risks.
- The Service Provider shall immediately notify SARS of any OEM announced security vulnerabilities, firmware flaws, or end-of-support risks.

j. Physical Security & Asset Handling

- The Service Provider shall ensure secure handling, storage, and transport of all SARS devices.
- A documented chain of custody shall be maintained for all device movements.
- Devices shall be protected against tampering, theft, or unauthorised access, including during transport and storage.
- SARS may require security escorts or enhanced physical controls for sensitive movements

i. Security Incident Management & Breach Notification

- The Service Provider shall immediately notify SARS of any:
 - Actual or suspected security incident
 - Data breach
 - Loss, theft, or compromise of a SARS asset
- Notification shall occur without undue delay and include:
 - Nature of the incident
 - Affected assets or systems
 - Immediate containment actions taken
- The Service Provider shall cooperate fully with SARS SOC, CSIRT, and forensic investigations.
- The Service Provider shall not communicate externally regarding any security incident involving SARS without prior written approval.

j. Monitoring, Audit & Assurance

- SARS reserves the right to audit the Service Provider's security controls, processes, and compliance at any time.
- The Service Provider shall remediate identified security findings within timeframes specified by SARS.
- Repeated or unresolved security findings may result in penalties, service credits, or contract termination

k. Business Continuity & Resilience

- SARS may request the Service Provider to assist with server infrastructure during Business Continuity and Disaster Recovery testing.

l. Termination & Data Return

- Upon termination or expiry of the Agreement, the Service Provider shall securely return or destroy all SARS data and assets.
- A formal data destruction attestation shall be provided to SARS

6 SERVICE DEFINITIONS AND REQUIREMENTS

A Service Provider appointed must provide all the services detailed in this paragraph 6 unless otherwise specified.

6.1 Service Management

The Service Providers appointed in Tower S will be required to maintain standards of service management and/or conform to best practice IT Service Management in their organisations dealing with the following processes:

- Incidents Management;
- Problems Management;
- Change and Release Management;
- Configuration Management;
- Service level management;
- Performance and Capacity management; and
- Service management reporting.

The Service Provider must hold an ISO certification (ISO 20000 – IT Service Management) OR a formal IT Service Management Maturity Assessment report showing an overall organisational Maturity score of 4 (quantitatively managed or equivalent) or higher.

The appointed service provider must have a well-established IT Service Management system/toolset that is automated to support the efficient and effective delivery of IT services to SARS. The automated system will have a ticketing and incident management module that allows for the automated creation, assignment, tracking of tickets, notifications and escalation based on pre-defined rules. The CMDB module should automatically keep track of the configuration items (CIs) in the IT infrastructure. The solution should allow for the automated creation, assessment, and approval of change requests. Furthermore, the automated system will have robust service management reporting and analytics capabilities. It should generate automated reports and dashboards, providing insights into various ITSM metrics, such as ticket volumes, resolution times, SLA compliance, and other performance indicators. This enables data-driven decision-making and helps identify areas of improvement.

The Service Provider must provide a 24x7 external web interface (e.g., a Contact or Service Centre) for the reporting of incidents and problems and to provide status updates. Service Providers are not required to interface directly with the SARS service management system, nor are they required to receive requests, respond to incidents or generally update records directly from the SARS service management system.

The Service Provider will be expected to participate, provide information and perform tasks as may be prescribed by the SARS PPS&G in terms of incident, problem, change, service level management, performance and capacity management.

The Service Provider will also be required to receive, route and update tickets on SARS's Service Management System. The Service Provider must provide as many personnel as SARS has provided licensing to work directly on SARS's Service Management System to receive, route and update tickets.

Should the Service Provider require additional licenses, it will be at the Service Provider's cost. The Service Provider may, in addition to this at its own cost, develop and implement an interface between the SARS Service Management System for incident management. SARS will co-operate with the Service Provider in developing such an interface, but SARS reserves its rights to make configuration changes as and when it sees fit to the SARS Service Management System and will give the Service Provider reasonable notice of its intended changes. Any costs relating to the hardware, software licensing, maintenance and configuration of the interface will be for the Service Provider.

Therefore, SARS recommends that the Service Provider determines the feasibility (number of incidents per month) to integrate during the Transition period since there are several factors to consider when integrating with SARS as per below:

- Hardware costs;
- Software costs;
- People costs being on standby and resolving technical issues, testing after changes on firewalls, network, servers, software, etc.;
- Security considerations exposing more interfaces, etc.; and
- Customisation/development costs.

The Service Provider will have the capability to log, receive, route and update tickets remotely without VPN services required during the Transition period. The Service Provider must ensure sufficient personnel are provided (remotely where required) to meet the contractual performance standards, including the Service Levels.

If the Service Provider receives sufficient incidents and there is a benefit to SARS and the Service Provider and it is viable to integrate, then the Service Provider should pursue the integration route.

Currently, the SARS standard for Service Management (Incident Management) integration is Web Services as per below:

- Enterprise Service Bus (Broker) and B2B Gateway (DMZ);
- Integration (Inter-Enterprise);
- Messaging (Queues) and Web Services;
- Async (Queues) and Sync (Web Service Calls);
- Request-Response;
- Integration Time: Near real-time;
- Message Multiplicity: Single Entity; and
- Message Size: Small.

Table C-1 sets out the number and type of SARS Service Management System licenses that SARS will make available to the Service Provider for Tower S. The Service Provider may, during the Term, with 30 (thirty) days' notice, request additional Service Management licenses. However, the Service Provider must note that the costs associated with such additional licenses will be recovered from the service provider.

Table C-1. SARS Service Management System licenses that will be made available per Service Management module for Tower S respectively

License type	Tower S
Change Management	1 X Service Management Suite Named
Configuration Management	1 X Service Management Suite Named
Incident Management	2 x Service Desk Named
Problem Management	1 x Service Desk Named
Release Management	1 x Service Desk Named

SARS reserves the right to change its service management system during the intended Term.

SARS will not provide permanent seating and provisions will be made during transition period for the Service Provider personnel performing service management services for Tower S.

The Service Provider must ensure that sufficient personnel are provided to meet the contractual performance standards, including the Service Levels, regardless of the number of Seats provided by SARS. The Service Provider must monitor the utilisation of the licenses and must submit a request to SARS for the increase/decrease of the number of licenses as and when required. SARS will review the request for the additional/reduced requirement and, if approved, adjust the provisioning accordingly within 30 (thirty) days from the date of the request. The Service Provider will not be excused from its obligations to meet the Service Levels if SARS is unable to meet the number of licenses that are requested by the Service Provider in excess of the numbers in Tables C-1. SARS will, on a regular basis, review the licenses across all services and functions by the Service Provider and if the number of licenses provided by SARS cannot be justified, SARS reserves the right to reduce the allocations accordingly.

6.2 Device-based Services

The applicability of the Device-based Services to categories of Tower S Servers is set out in paragraph 10.

6.3 Service Descriptions

The Services are set out at a high level in this document and must be read together with the provisions set out in the statements of work in the Server Device Support Services Agreement, in particular Schedule B (Service Management Services SOW); Schedule B-S (Server Support Services SOW)

The Bidder will be required to compile detailed operational procedures based on the requirements set out for the various device categories during Transition. The Bidder must reference the relevant provisions in Schedule B (Service Management Services SOW); Schedule B-S (Server Support Services SOW); Server Device Support Services Agreement for a detailed description of the obligations required during Transition.

6.4 General obligations applicable to all Device-based Services

The Bidder must take special note of the service management-related activities set out in the Schedules listed above, which are applicable to all the services described hereunder. The Bidder must include these service management activities in its costing and pricing for the services.

6.5 General housekeeping activities

Unless specifically excluded, general housekeeping activities must be performed every time the Service Provider is required to perform either a repair or Standard Chargeable Service. These activities must be included in the Bidder's costing and pricing for the services. The general housekeeping activities must include at a minimum:

- Verifying the condition of the server device;
- Specifying any visible damage or defect to the server device in the call closure report;
- Verifying that the asset tag and serial number is recorded correctly in the SARS CMDB and securely attached to the server device;
- Verifying the asset information (server device description; room number, user/owner information, etc.) and updating the information if needed;
- Basic cleaning of the device and the device's immediate environment;
- Verifying that the installation and placement of the server device and related equipment does not place the device, related equipment or personnel at risk, for example, loose cabling;
- Advising the user as to the device's operation and placement, including any such items noted in the call closure report.
- Verifying that users can access network applications by confirming that all necessary connections, including cables, wireless configurations and network peripherals are securely connected and properly configured before call closure;

- Identifying and addressing potential issues or areas requiring preventive maintenance;
- Verifying that all components and peripherals attached to the server device are functional and operating before the call is closed;
- Obtaining the user's signoff that the device is fully operational and housekeeping activities checklist was conducted; and
- Logging/assigning an incident and/or problem ticket for repair or other services outside the scope of the Service Provider's contracted services that are ascertained to be required during the performance of housekeeping activities.

6.6 Break-fix Service Descriptions

The services described below represent the different Break-fix services that are required to be provided by the Service Provider. The Break-fix services that are required for the device categories are listed in Table S-2 for Tower S. The Bidder will be required to provide rates for the different Break-fix services and SARS will elect which Break-fix service will be applicable to specific models of equipment.

For example, the Bidder must provide pricing for Break-fix In-warranty services for server devices. SARS may elect to receive Break-fix In-warranty services for device equipment that is still under warranty.

SARS may elect to receive Break-fix In-warranty services for device equipment that is still under warranty and pay the monthly per In-warranty server device Break-fix fee for its devices that are under warranty. Out-of-warranty, Out-of-support devices must be managed on Time and Material basis.

Break-fix services include the restore of the device to its last working configuration.

6.7 Break-fix services required for devices under warranty

The Break-fix services required by SARS include services to be performed for server devices that

- (1) Have been procured with a warranty period, during which defects will be repaired free of charge and such devices are still within the warranty period; or
- (2) Are covered by a repair contract from a third party.

These devices will be categorised as "**In-warranty**" devices.

During Transition, the Service Provider will be required to establish and/or verify the warranty status of all in-scope server devices. The presumption will be that a device is under warranty (and therefore will be classified as an In-warranty device) unless the Service Provider can provide reasonable evidence to the contrary to SARS.

SARS may extend the warranty contract with the OEM to ensure the availability of spares and to guarantee the repair of critical devices. Where such arrangements have been made for an Out-of-warranty device, such device will be regarded as an In-warranty sever device and the In-warranty rate will apply.

The Service Provider must protect SARS's investment in such warranties by ensuring that repairs are carried out in a way that maximises the advantage of the warranty conditions and not do anything that would prejudice the warranty conditions that SARS procured with such devices.

Regardless of such arrangements, the Service Provider must provide the necessary service management, co-ordination and other required services to effect the repair under the terms of the warranty from the warranty provider or under the terms of the repair contract from the third party.

6.8 Break-fix Services Required for Devices not Under Warranty

The Bidder is required to provide Break-fix services for server devices that are not under a warranty and that are not the subject of a third-party repair contract from a warranty provider. These devices will be categorised as “**Out-of-warranty**” devices.

For Out-of-warranty server devices, the Bidder must manage these devices as Time and Material and provide full Break-fix services. The Bidder must, therefore, include the cost of all activities, parts, labour, etc. to effect repair of the device.

If the cost to repair an Out-of-warranty server device, for which the Service Provider is obligated to repair for the monthly charge, will be greater than 60% of the replacement cost of the device, the Service Provider must inform SARS that the device is “**Uneconomical To Repair**” and SARS may elect to replace the device at its own cost. For clarity, the cost to repair refers to a single incident and not the accumulated repair cost for a server device over its lifetime. If the Service Provider must provide a Whole Unit Spare (WUS), the Service Provider must provide and leave the WUS in place for 45 (forty-five) days or until SARS provides a replacement device, whichever occurs first. After 45 (forty-five) days, the Service Provider may remove the WUS, whether SARS has provided a replacement device or not. The installation of the replacement device provided by SARS in the place of the UTR device must be made by the Service Provider at no additional charge to SARS.

6.9 Break-fix Services for Server Devices that Require only the Facilitation of Repair (Exclude actual repair activities)

For this category of server devices, the Service Provider will be required to perform the service management and all co-ordination activities to facilitate the repair, including the sourcing of a certified repair provider, and activities to re-install the repaired server device. These devices will be categorised as “**Service-only**” server devices.

The Service Provider must engage an OEM certified repair provider(s) for the repair of the server device, obtain quote(s) and submit all relevant information and the quote to SARS for approval. On approval the Service Provider must co-ordinate all activities to have the server device repaired, including making payment to the repair provider. The Service Provider will then submit an invoice to SARS for the cost of the repair at no markup. SARS may elect to nominate a repair provider, in which case the Service Provider will co-ordinate all repair activities with such repair provider.

In determining the rates for Service-only server devices, the Bidder must exclude the actual cost of the repair of the device from the monthly rate.

6.10 Break-fix Services that Qualify for Permanent Replacement

For this category of server devices ("**Swap-out**" devices), the Service Provider must permanently replace faulty server devices from a pool of SARS-provided Swap-out units. If of an incident affecting a device in the category for which a Swap-out service has been selected by SARS, the Service Provider must diagnose and attempt to repair the affected device. If the fault in the affected device cannot be rectified by the Service Provider, the faulty device must be permanently replaced with a functioning server device from the pool of SARS-provided Swap-out units. All other activities must be performed, including the updating of the SARS CMDB with the details of the Swap-out server device and the faulty server device. The faulty server device must be returned to SARS.

The Swap-out service can only be provided using Swap-out units from a SARS-provided pool and any unit used to Swap-out a faulty server device must be a SARS asset. The Swap-out service is not to be confused with the WUS service, which *temporarily* replaces a faulty server device with a functioning server device while the faulty server device is being repaired.

The process of taking on SARS-provided Swap-out units will be defined and undertaken during Transition. The number of Swap-out units to be provided by SARS for the Swap-out pool will be determined as part of the Transition project and will take into consideration the distribution of units deployed, the manufacturer specifications for mean time to failure, and industry guidelines for spares pools.

6.11 WUS Services

The WUS service is not a service provided on its own but is provided as an option in conjunction with the In-warranty, Out-of-warranty and Service-only Break-fix services. The Break-fix service descriptions for each server device category specify whether a WUS service must be provided (either Service Provider provided or SARS-provided as per the service description). If a Wus service is specified, the Bidder must include the cost to provide a WUS in the related monthly rate.

6.12 Summary of Break-fix Services and Related Process Flows

The purpose of the process flow diagrams in Attachment A is to highlight major differences between the different processes and must not be taken as a comprehensive list of activities that have to be performed by the Service Provider. The process flow diagrams will be used as the basis for the process design to be documented by the Service Provider during Transition.

Table C-3 Break-fix service process flow diagrams

Break-fix service process flow diagrams	
In-warranty where a WUS is not applicable	Attachment A Diagram 1.1
Service-only repair where a WUS is not applicable	Attachment A Diagram 2.1
SARS-provided WUS process	Attachment A Diagram 3.1

6.13 Standard Chargeable Services

Standard Chargeable Services must be provided on request by SARS. Bidders must provide pricing for the Standard Chargeable Services as listed and described below. In addition, Bidders must provide volume-based pricing for Standard Chargeable Services for volumes with the assumption that all these volumes will be on same site per request.

SARS may request a quote for a project to perform such standard services across multiple devices. It is expected that the quote for a project to perform these services across multiple server devices will be less than the aggregate of the Standard Chargeable Service charges if SARS was to request them individually per server device. It will be at SARS's sole discretion to accept the quote for the project or to make individual requests for the Standard Chargeable Service to be performed for each of the server devices. Server devices that are not recorded on SARS's CMDB but that falls into the categories of SARS may increase the take-down annual limit during the Term and the pricing structure for additional take downs must be given.

Rates for the Standard Chargeable Services must be submitted by the Bidder for each Site Classification (Metro, Town or Rural).

Table C-4 Summary of Standard Chargeable Services and related process flows

Standard Chargeable Services	
Installation/Replacement Process	Attachment A Diagram 4.1 The Service Provider may be expected to attach a SARS barcode as part of the Installation/Replacement process.
Move	Attachment A Diagram 5.1 Moves within a building, the Service Provider must perform the transport of the device at no extra charge and without any pass-through costs to SARS.
Decommission for Disposal	Attachment A Diagram 6.1

Expedited Service Request	On request by SARS: • Provide SARS with a commitment to the best possible time to respond/repair a device. • On acceptance of the expedited commitment, perform accordingly. • Obtain signoff from a SARS representative. • Submit invoice for Expedited Service Request. An Expedited Service Request will only be charged on a request being made by SARS and the committed time to respond/repair being accepted by SARS. (No process flow diagram is presented for Expedited Service Requests)
Delivery Acceptance Test	Attachment A Diagram 7.1 The Service Provider may be expected to attach a SARS barcode as part of the Delivery Acceptance process.

6.14 Miscellaneous Services

SARS may, from time to time during the Term, request miscellaneous services as set out in Table C-5. Where the Service Provider quotes for such services in response to a request by SARS, such quote must be made using the personnel rates submitted in the Service Provider's Proposal and the number of hours and personnel skill level quoted must be substantiated in full.

Table C-5 Summary of Miscellaneous Services and Related Process Flows

Miscellaneous services	
Secure Courier Service	On request by SARS: • Provide a quotation for the secure transportation of devices, including the insurance of the devices (the risk of loss of damage will be borne by the Service Provider while the device is under the Service Provider's care or possession). • On acceptance of the quotation by SARS, perform the courier service. • Invoice SARS as per the proposal, either on the completion of milestones or otherwise as agreed in the proposal. Service Provider to update the CMDB. Asset Management

Miscellaneous services

Asset Tracking: The courier service should have a robust system for always tracking the location and status of assets. Full live Tracking of devices in transit with full audit trail available at all stages.

Delivery Confirmation: The courier service should provide proof of delivery, such as signed receipts or digital confirmation.

Asset Valuation: The courier service should note and use the replacement valuation of assets for insurance purposes.

Packaging

Asset Protection: The courier service should have measures in place to protect assets from damage during transit. This includes proper protective packaging, handling, and transportation procedures.

Protective Packaging: This serves as a shield for products, safeguarding them against potential hazards during transportation. It acts as a buffer, absorbing shocks, and vibrations, and protects against environmental factors.

Damage Prevention: The Bidder should ensure that damage prevention and proper packaging are included. Proper packaging significantly reduces the risk of damage caused by mishandling, collisions, or drops during transit. Protective packaging also acts as a barrier against moisture, dust, and dirt to preserve the item's quality, functionality, and appearance.

Security Provided

Secure Delivery: The Bidder should ensure that the package arrives safely and securely at its destination. This includes tamper- and damage-proof packaging, authentication protocols, real-time tracking, and confidentiality.

Transparent, End-to-End Surveillance: Secure courier services should be painstakingly thorough and cautious throughout both the shipping and delivery process. This means tracking all key points along the way: pick up, drop off, and shipping route.

Miscellaneous services	
	Identity Verification: The Bidder should ensure that verification of recipient's Identity is done to ensure they are delivering items to the correct person. Physical Security: The Bidder should ensure that the equipment can be transported with armed security for large shipments between sites on request. Integration with Warehouse Services The Bidder should ensure that their transport services are integrated into their warehousing solution
Project Service	On request by SARS: • Provide a quotation for Project Services • On acceptance of the quotation by SARS, perform the project service. • Invoice SARS as per the proposal, either on the completion of milestones or otherwise as agreed in the proposal. Service Provider to update the CMDB.

For clarity, the table below sets out the responsibilities of certain services applicable to Tower S with the high-level responsibilities expected of the Service Provider and the basis on which the Service Provider is engaged. The purpose of Table C-6 is to provide clarity to the boundaries of scope and does not set out to describe the full scope of services.

Table C-6 High level division of responsibilities to Tower S

Scope		Responsibilities	
		Service Provider	SARS
	Incident detection, filtering, correlation, first line diagnosis and first line repair activities.	If, as part of standard housekeeping tasks, an incident is detected it must be reported to SARS.	SARS monitors all elements of the network and receives calls at the ICT Service Desk and IT Operations Centre. First line diagnosis and remote rectification activities.
	Open ticket and route to support group.	Where required or directed by SARS.	Open ticket on SARS Service Management System. If related to a failure on a server device within the scope of services, route to Service Provider.

Device-based Services	Receive ticket.	Service Provider must receive the ticket from the SARS system.	
	Perform onsite diagnosis and repair/Swap-out	Service Provider must confirm server device is functioning, it is on SARS' network, and that the SARS support teams can remotely access the device.	
	Close ticket	Service Provider must place the ticket into resolved status on the SARS system.	SARS closes the ticket.
	Release management	Adhere to SARS release management PPS&G. Manage and/or participate in a release as and when required.	Manage and support release management process.
	Change management	Adhere to SARS change management PPS&G. Manage and/or participate in a change as and when required.	Manage and support change management process.
	Problem management	Adhere to SARS problem management PPS&G. Manage and/or participate in a problem investigation and remediation as and when required.	Manage and support problem management process.
Standard Chargeable Services	Pre-production Preparation/ Staging	Perform on request by SARS	Initiate request
	Installation		Initiate request
	Replace		Initiate request
	Move		Initiate request

Scope		Responsibilities	
		Service Provider	SARS
	Add/Change		Initiate request
	Decommission for Re-use		Initiate request
	Decommission for Disposal		Initiate request
	Expedited Service Request		Initiate request
Other Services	Secure Courier Service	On request by SARS: provide quote at standard rates; on acceptance, perform courier services.	
	Projects (including Project Management)	On request by SARS: provide quote at standard rates and on acceptance execute the project.	Initiate request
	SLA Management	Perform on continuous basis.	
	Capacity Management	On request by SARS: provide information.	Perform
	Availability Management		Perform
	Performance Management		Perform

6.15 Service Provider Management Personnel

The Service Provider must provide an Account Executive/Service Delivery Manager, and Operations Manager. The Operations Manager must maintain a presence and actively monitor and manage the delivery of Service during office hours, service outages and extended office hours as required during SARS high focus and/or peak periods at SARS Head Office in Brooklyn, Pretoria. The Account Executive/Service Delivery Manager and Operations Manager will be designated as Key Service Provider Personnel (see Server Device Support Services Agreement for the definition and conditions relating to the appointment and replacement of Key Service Personnel and the requirement for SARS to approve such appointments). For Tower S, the Operations Manager will be one person with multiple roles. Operations Manager should not be deployed to perform technical functions.

SARS will not provide permanent seats for Service Provider onsite management personnel for Tower S respectively.

SARS requires the availability of Key Service Provider Personnel for regular meetings to be held at SARS's request at SARS premises. SARS may also require the presence of Key Service Provider Personnel at ad hoc meetings at SARS'S premises with reasonable notice. Reasonable notice will be determined considering the urgency with which the subject matter of the meetings is to be addressed.

In addition to the requirements specified in the Server Device Support Services Agreement, SARS requires the Account Executive/Service Delivery Manager and Operations Manager to hold positions of sufficient authority within the Service Provider's organisation to provide an effective escalation point for issues that may arise during the Term. The Service Provider's Account Executive/Service Delivery Manager and Operations Manager must have a good understanding of the principles of service management and must preferably hold an ITIL certification.

6.16 Project Support

As and when required by SARS, the Service Provider will be required to provide *ad hoc* project management support for the roll-out of projects. The engagement of the project management support must be provided by the Service Provider at the Personnel Rates submitted by the Service Provider in its Tower S Pricing Response Template.

6.17 Consulting

The Service Provider will be required to provide SARS with *ad hoc* advisory services related to the Services at no additional charge.

Formal consulting assignments may be engaged on a paid-for basis at the consulting rates as provided in the Service Provider's Proposal. Formal paid-for consulting assignments may only be provided after specific written authorisation by SARS to the Service Provider.

6.18 Training

The Service Provider will not be required to provide formal training to SARS personnel as part of the base services.

SARS may also contract the Service Provider to provide training as part of a Project on a Time and Materials basis.

6.19 Administration

The Service Provider will be required to perform administrative activities that are obligatory for the effective delivery of the Services as detailed in this Business Requirements Specification and the Server Device Support Services Agreement which include:

- Effective management of meetings (schedule, agenda, attendance register, minute etc.);
- Information management (maintain equipment lists, site lists, standby lists, etc.);
- The production and distribution of reports: annual, weekly, monthly, daily and *ad hoc* reports as required by the contract, as specified by SARS during Transition and otherwise as reasonably required by SARS; and

- Ticket completion (updating of all relevant documents and systems, e.g. the CMDB, invoicing etc.).

The Service Provider must take note of the obligation regarding SARS's Oath of Secrecy screening and vetting obligations to be performed for Service Provider personnel in the Server Device Support Services Agreement.

7 RESEARCH AND DEVELOPMENT

In the constantly advancing technological environment, it is imperative for our organisation to commit to research and development efforts to maintain a competitive edge and optimize the utilisation of tools, systems, and hardware investments within SARS. To accomplish this objective, the Service Provider is required to provide the necessary resources and support to facilitate innovation and exploit contemporary technologies for SARS' advantage, in accordance with SARS's requirements and strategic objectives. This involves the provision of hardware, software, and expert personnel to strengthen state-of-the-art research and development proof of concepts and technologies. By fulfilling these obligations, the Service Provider enables SARS to investigate innovative concepts, evaluate pioneering methodologies, and validate technological suitability and value within the SARS context. As part of the research and development services, Bidders are expected to provide expertise and recommendations.

8 TRANSITION PROCESS

8.1 Transition Plan

The Service Provider is expected to provide a transition plan that contains key elements for a transition project to achieve a successful transition and minimise disruptions and not compromise services to SARS. The transition plan for the appointed Service Provider should clearly elaborate on the following aspects:

- Projects Phases: Clearly stipulated stages of the transition project (e.g., Initiation, Planning, Execution, Monitoring, Closure);
- Project Management: The Project schedule for the transition process with scope, timelines, dependencies, milestones, deliverables, based on the services provided in Tower S and showing a maximum transition period of 3 (three) months,
- Roles and Responsibilities to be defined by the appointed Service Provider, SARS and the outgoing Service Provider,
- Stakeholder Engagement and Communication: Approach of managing identified stakeholders and maintaining regular and effective communication channels to keep stakeholders informed throughout the transition process,
- Risk management: Management of identified risks and issues associated with the transition process and mitigation strategies,
- Deployment approach and Migration: Clearly outline the deployment approach, implementation and migration to move services to the appointed Service Provider and specify how downtime and disruptions will be minimised during the transition,

- Training and Knowledge Transfer: Outline training approach and mechanisms of knowledge transfer,
- Quality assurance: Approach and processes to reduce or eliminate errors or defects in the final outcomes of a project establishing standards, guidelines and procedures to prevent quality issues and maintain the integrity of the product or service throughout its development,
- Compliance and Governance: Ensure compliance with relevant regulations and industry standards: and
- Post-transition Support and Optimisation, provide ongoing support and maintenance for the new infrastructure/services following the transition.

8.2 Experienced Transition team

For the transition process, the appointed services provider is required to have multidisciplinary transition team with experience in executing a transition project similar to the size of SARS. The different roles in the transition team structure should fulfil the following areas of expertise at a minimum, supported by relevant experience: Transition Management, Project Management/Program Management, Vendor and Contract Management, IT Service Management and Technical Subject matter experts.

9 TOWER S: SERVER SUPPORT SERVICES

9.1 Scope

The scope of SARS's requirements for Tower S: Server Support Services comprises nationwide provision of the following:

- Server support services (Device-based Services, Standard Chargeable Services, project, consulting, body-shop engineers and training) for SARS-owned and SARS-managed Dell Intel-based Servers, Dell Blade servers, Dell Chassis, including hardware support. SARS has standardized on one Server brand namely Dell. Service Providers must support this brand. This includes having the necessary OEM accreditation to provide comprehensive support for this brand, ensuring that the Service Provider's team is ready to offer proficient hardware and parts assistance.

The successful Bidder will be expected to ensure that their staff are fully trained and up to date with the necessary skills to support the Server brand, reflecting a commitment to ongoing professional development and certification in line with the latest technological developments. Furthermore, the Service Provider is expected to guarantee a supply of genuine parts and accessories for this Server brand, ensuring swift and effective responses to service requests. This also involves proactive engagement with the OEM to stay abreast of technological updates, ensuring that SARS benefits from high-quality, secure server solutions. This approach aims to uphold a robust, efficient server environment tailored to meet SARS's specific operational requirements and security protocols.

- Procurement and other services
 - Non-exclusive procurement of Server consumables not limited to OEM, including pre-sales and post-sale support from OEM Partners' supply of consumables.
- The common services set out in paragraph 6, including service management, Service Provider management personnel, administration, consulting, project management and support.
- The services will comprise:
 - a. The management of incidents,
 - b. The provision of defined services relating to the supported equipment and maintenance services;
 - c. Professional services,
 - d. The provision of Standard Chargeable Services such as installs, move, add, change and decommissioning services; and
 - e. Compliance with required service management procedures.

The required services include Professional Services, to provide for escalation of DELL OEM hardware and software related incidents and configuration related incidents.

As part of Device-based Services in Tower S, the Service Provider must:

- a. Ensure that the server device operating systems are supported, In-warranty and all OEM-recommended firmware are installed in line with SARS PPS&G,
- b. Inform SARS of any announcement made by the device OEM regarding hardware, firmware and software end of support dates,
- c. Follow the SARS service management procedures to ensure that the servers are maintained in accordance with the SARS PPS&G; and
- d. Resolve operating system software incidents as part of the Break-fix services.
- e. SARS may require the Service Provider to perform inventory checks.
- f. SARS may require the Service Provider to provide courier services.

SARS may request Body-shop engineers during the term of the contract, new rate cards per skill level will be included as part of Professional Services and extend the services to server administration and management.

Professional Services (server-based) must include skills for Microsoft Azure Cloud Services and OEM server devices as and when required during the term of contract.

The Service Provider must provide Research and Development Services — provide recommendations towards new technologies and automation in server space as and when required.

9.2 Flexible Support Services

The Service Provider shall be required to provide flexible support services to accommodate SARS's changing needs and requirements concerning the support of evolving technologies and business demands.

9.2.1 Adaptive Service Delivery

The Service Provider shall demonstrate the capability to expeditiously adapt to SARS's varying needs by delivering prompt and efficient support services in response to fluctuating demands, technological progress, and shifting business requirements. This includes, but is not limited to, the deployment of supplementary resources, the reallocation of existing resources, and the modification of support processes and procedures as necessary.

9.2.2 Proactive Technology Support

The Service Provider shall proactively monitor and stay informed about advancements in technology and industry best practices to ensure that SARS receives adequate support. This includes providing guidance and recommendations for the adoption of new technologies, upgrading existing systems, and optimising the overall IT infrastructure.

9.2.3 Scalable Support Model

The Service Provider shall implement a scalable support model capable of accommodating the growth, expansion and reduction of server devices of SARS's IT infrastructure and services. This includes the ability to adjust support levels, resource allocation, and service offerings as needed to meet SARS's evolving demands and requirements.

9.2.4 Agility in Service Implementation

The Service Provider shall be capable of rapidly implementing new services, processes, or support structures in response to SARS's shifting needs and requirements. This includes the ability to efficiently integrate new technologies, systems, and solutions into the existing IT environment, while ensuring minimal disruption to SARS's business operations by conforming to the service management frameworks.

9.2.5 Collaborative Approach

The Service Provider shall work collaboratively with SARS to understand its changing needs and requirements and develop and implement effective support strategies accordingly.

This includes maintaining open lines of communication, actively seeking feedback, and continuously refining support processes and procedures to ensure optimal service delivery.

9.3 Delivery Model

SARS currently engages a single Service Provider to provide server support services. The incumbent Service Provider is managed by SARS and provides the scope as described above. SARS's requirements for services in this Tower S now include additional services such as the inclusion of support for additional device types.

9.4 Transition

The Service Provider appointed in Tower S is required to complete the Transition Services within 90 days from the Effective Date. By the end of the 90 days, the Service Provider must have assumed full management responsibility for the full scope of Server Support Services. In addition to any other commitment required in the Server Device Support Services Agreement, the Service Provider must have:

- Fully designed, developed, implemented the signed-off processes, procedures, schedules and work practices detailed in the Server Device Support Services Agreement, especially those detailed in Schedule B-S and its attachments;
- Verified the warranty status of all Server Devices,
- Committed to reporting and meeting Service Levels as set out in Schedule C and Appendices C-S-1 and C-S-2 of the Server Device Support Services Agreement.
- Determined and defined the method of obtaining the data from the SARS Service Management System, including the assignment of Service Provider personnel to perform transactions on the SARS Service Management System and, if the Service Provider has so elected, to interface its own service management system with the SARS Service Management System,
- Established the required governance as specified in Schedule E of the Server Device Support Services Agreement.
- Taken over the management of any server support services that are sourced through third parties; and
- Attended any training specified by SARS to understand the SARS environment, systems and operating procedures.
- The Service Provider is not expected to conduct an audit of the devices to be supported. The SARS CMDB will be used as the basis for determining the devices that will form the scope of the Services and for the purposes of billing. If an incident is logged for a device that is not recorded on SARS's CMDB but falls into the categories of supported Server devices, the Service Provider must attend to the incident on a time and materials basis. The Service Provider must record all relevant information relating to the device that will enable the device to be recorded on SARS's CMDB

and the device will thereafter be deemed to be covered in the support agreement and the Service Provider may thereafter charge for the device according to the rate corresponding to the device's classification. No Service Levels will apply to the restoration of service relating to devices that are not recorded on SARS's CMDB. In the event the Service Provider becomes aware that a device on SARS's CMDB is no longer deployed, it is incumbent on the Service Provider to inform SARS as soon as it has become aware of the device's status.

9.5 Device-based Services Applicable to Tower S

SARS has defined the various Device-based Services to be performed in general in paragraph 6.2 above. The categories of server equipment within the scope of Tower S are set out in Table S-1 below. Table S-2 sets out the Break-fix services that are applicable to the various categories of server equipment with reference to both Table S-1 and paragraph 6.2.

The details of the number of units, in each category, the number at each site in SARS and models are provided in the equipment lists included in the RFP pack.

- Tower S Site Classifications.
- Tower S Server Categories and Quantities; and
- Tower S Server Categories per SARS Site.

One of the objectives in this RFP is to achieve flexibility in the procurement of services. In this regard, Table S-2 sets out the Break-fix services that SARS may require during the Term. The Bidder is required to provide rates for all required services for each server device category set out below, as well as the rates for different Service Levels, Service Coverage Period and Site Classification of the devices. The Bidder is referred to the Tower S Pricing Response Template for the details of prices that must be supplied by the Bidder.

During contract finalisation, SARS will make an election in each device type as to which Device-based Service must be provided as of the Commencement Date. Thereafter, SARS may change the Device-based Service applicable to a type of device with 2 (two) months' notice.

For example, the Bidder must provide rates for Break-fix services (In-warranty, Out-of-warranty, Swap-out and Service-only) for KVM Consoles. SARS may elect during contract finalisation to contract for Break-fix services (In-warranty) and Break-fix services (Out-of-warranty) for this type of device. Within 2 (two) months' notice SARS may change the services applicable to this type of device (and the applicable Charges) to be Swap-out services.

Table S-1: Categories and Types of Servers and Server Equipment

Category	Description / notes
Server Computing Devices	
Server (Intel) Dell PowerEdge R710 Dell PowerEdge R720 Dell PowerEdge R730 Dell PowerEdge R740XD Dell PowerEdge R740 Dell PowerEdge R760 Dell PowerEdge R910 Dell PowerEdge R920 Dell PowerEdge R930 Dell PowerEdge R940 Dell PowerEdge R960 Dell PowerEdge R240	Includes the Server, motherboard, firmware, case, power supply, memory, hard drives, Host Bus Adaptor (HBA), network card, and SFPs. Note that this excludes the display/screen.
Server Blade (Intel) Dell PowerEdge M630 Dell PowerEdge M640 Dell PowerEdge MX740C Dell PowerEdge FC640 Dell PowerEdge MX750C Dell PowerEdge MX760C	Server blade including firmware.
Blade Chassis (Intel) Dell Blade Enclosure FX2 Dell Blade Enclosure M1000e Dell Blade Enclosure MX7000	Includes the chassis, chassis management controller, SD cards, power supply, switches and backplane.
Server (Shared infrastructure platform)	Shared infrastructure server platform that integrates processor, network switches,
Server Peripherals/Miscellaneous	
KVM Console	KVM console and keyboard for server rack configuration.
KVM Switch	KVM switch for multiple server management.

Table S-2: Detailed Description of Device-based Break-fix Services Applicable to Server and Server Equipment Categories and Types

Category/type	Break-fix Services				Notes
	In-warranty	Out-of-warranty	Time and material	Swap-out	
Server Computing Devices					
• Server (Intel) • Server Blade • Blade Chassis (Intel), including onboard switches • Server (shared infrastructure platform)	SP-provided WUS	SP-provided WUS	n/a	n/a	All devices must be repaired onsite unless authorised by SARS. The Service Provider must provide a WUS to meet the Service Levels. Note that in practice the WUS may be used to Swap-out parts to restore service while the faulty units are being repaired.
Server Peripherals / Miscellaneous					
KVM Console	No WUS	No WUS	SARS-provided Swap-out device	n/a	All devices may be repaired on or offsite.
KVM Switch	No WUS	No WUS	SARS-provided Swap-out device	n/a	All devices may be repaired on or offsite.

9.6 Service Coverage Periods and Service Levels Applicable to Tower S

The specific Service Coverage Periods applicable to the Break-fix activities in Tower S are set out in Table S-3 below. Note that the Service Provider must comply with the applicable change control authorisations when making changes to resolve incidents. Where the Service Provider is prevented by the SARS change management process from performing Change/Break-fix services within the times required to meet the Service Levels, the Service Provider will be excused from its obligations to meet the Service Levels in the instance. Regardless of the Service Coverage Period specified applicable to a device, if SARS's change management process requires Change/Break-fix activities to be performed outside the Service Coverage Period specified for a device, the Service Provider must perform such activities at the time required by the SARS change management process.

If, to restore services to a Device, the Break-fix activities required include the need to backup and/or restore user data from/to the Device, the time taken to perform the

backup and/or restore activities will be excluded from the elapsed time for the purpose of calculating Service Levels.

Table S-3: Service Coverage Periods applicable to Tower S – Business to determine sites — access constraints

Service Coverage Period	Period Covered
Basic	06:00 to 19:00 on weekdays regardless of whether the weekday falls on a public holiday or not.
Standard	06:00 to 21:00 on all days, including Saturdays, Sundays and public holidays.
Extended	06:00 to 00:00 on all days, including Saturdays, Sundays and public holidays.
Premium	24x7x365 (at all times).

The specific Service Levels applicable to the Break-fix activities in Tower S are set out in Table S-4 below and must be carried out within the principles listed below.

In all cases, the Service Provider must obtain authorisation to commence Break-fix activities.

When authorisation is received from SARS to commence service restoration activities at a particular approved start time, then service restoration must be completed within the number of hours indicated in Table S-4, according to the Service Level Class of the malfunctioning device, as measured from the approved start time. A standard 8 (eight)-hour service restoration will apply if service level classes cannot be met.

The exact guidelines expanding on the above principles will be documented during Transition.

The detailed operation of Service Credits relating to Service Level failures is set out in Schedule C of the Server Device Support Services Agreement.

Table S-4: Service Levels applicable to Tower S**Break-fix Service Level Classes**

Service Level Class	Time to Repair including parts
Bronze	Service restoration within 12 (twelve) hours of the ticket being assigned to Service Provider.
Silver	Service restoration within 8 (eight) hours of the ticket being assigned to Service Provider.
Gold	Service restoration within 4 (four) hours of the ticket being assigned to Service Provider.

Standard Chargeable Services Service Levels

Service	Time to Complete
Device IMACD	(One) 1 working day (completed on or before the same time of day as the request was made to the SP on the next working day). If the request was made on a non-working day, the request will be regarded as having been logged at the start of the next working day.

9.7 Service Provider Technical Personnel

At Commencement Date and throughout the Term, Service Provider technical personnel assigned to the SARS account must be in possession of the following minimum qualifications and experience when dealing with the corresponding technologies/services:

Device category/ Equipment type	Service Provider Personnel Required certifications/experience
Server Computing Devices	OEM certification with relevant years of experience CompTIA A+, N+, Server+ certifications; MCP (Microsoft Certified Professional) or Microsoft Certified Administrator Associate – Server) qualification with relevant years of experience
General Computer Device Engineer	OEM certification and Microsoft server certification with relevant years of experience
Project Management Services	Project Management Certification with relevant years of experience

Generally, all technical personnel must be familiar with basic service management processes, preferably a foundational level qualification. The Service Provider must ensure that for each SARS site, a qualified server engineer is able to provide services for the equipment located at that SARS site within the specified Service Levels.

The Service Provider must ensure sufficient personnel are provided to meet the contractual performance standards, including the Service Levels, regardless of the number of Seats provided by SARS. The Service Provider must monitor the utilisation of the Seats and must submit a request to SARS for the increase/decrease of the number of Seats as and when required. SARS will review the request for the additional/reduced requirement and if approved will adjust the provisioning accordingly within 30 (thirty) days from the date of the request. The Service Provider will not be excused from its obligations to meet the Service Levels due to an inadequate number Seats available to the Service Provider during the Term.

ATTACHMENT A: PROCESS FLOW DIAGRAMS

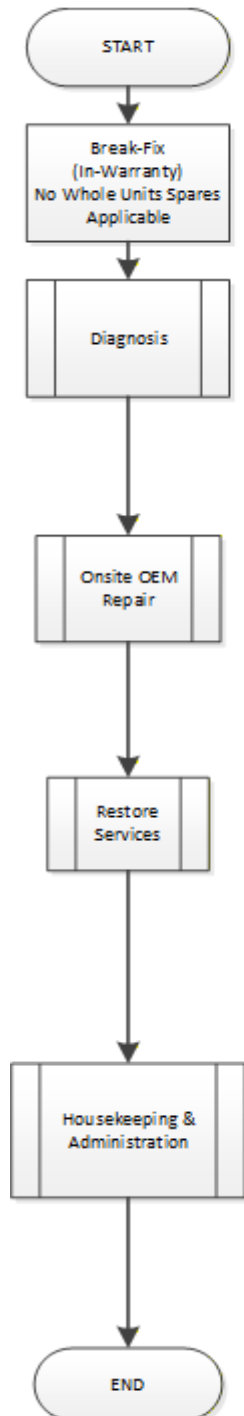
The process flow diagrams set out in this Attachment are set out to provide high-level guidance to the Bidder and do not contain all activities required for every process.

The Bidder must read these process flow diagrams in conjunction with provisions set out in *Schedule B of the Server Device Support Services Agreement* and this *Business Requirements Specification* and supplement them with any activities that are regarded as necessary in terms of industry best practice to meet the required outcomes.

The Bidder must include all activities as described above in its costing and pricing for the services. It is the obligation of the Bidder to transparently reflect all activities, both from the diagrams and supplementary additions, in the costing structure, leaving no room for future financial uncertainty. Where an activity is not relevant to Tower S. The process flow will be reviewed and finalised during the Transition.

1. IN-WARRANTY BREAK-FIX PROCESS (WUS NOT APPLICABLE)

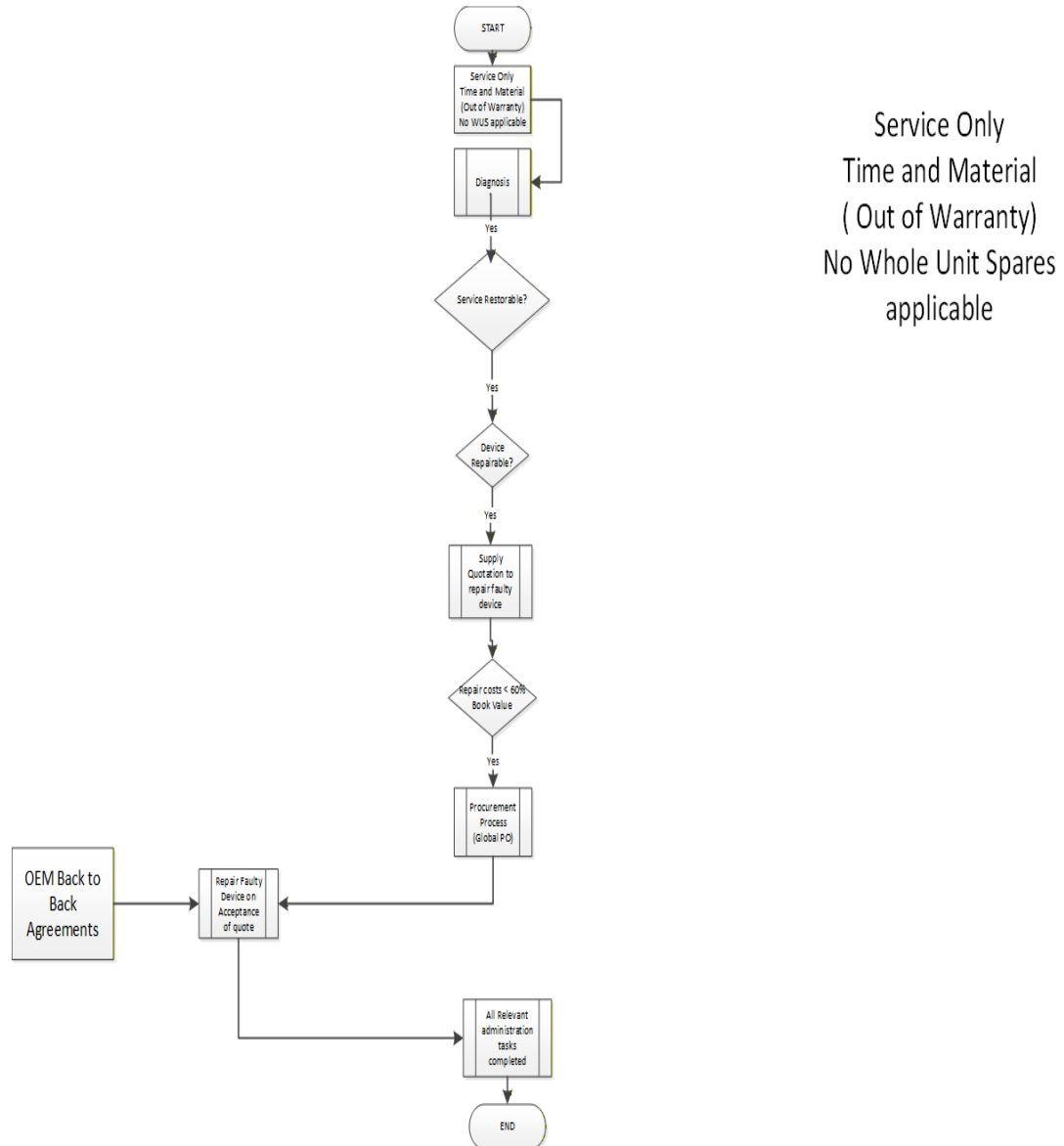
The flowchart set out immediately below describes the process to be followed for the repair of In-warranty devices that are required to be repaired onsite (Carry-in to OEM Repair only on SARS approval), where no WUS is applicable. The Bidder must supply a monthly price to facilitate co-ordination of warranty repair. No additional charges are payable by SARS to effect the repairs other than the monthly rate.



**Break Fix (In Warranty) No
Whole Unit Spare/Parts
Applicable**

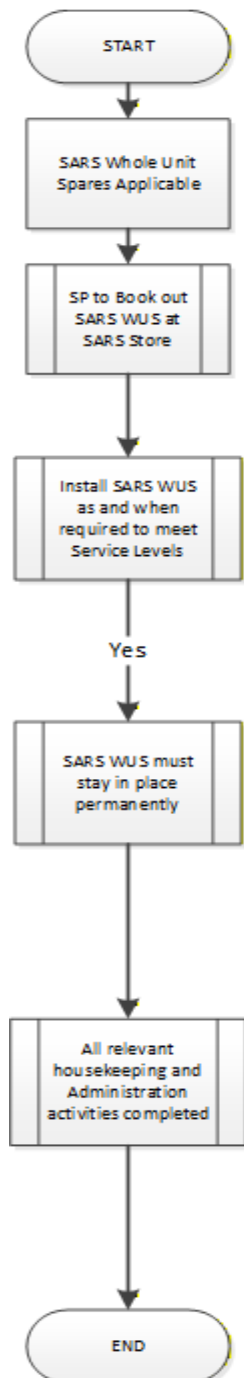
Diagram 1.1 Break Fix (In warranty)**2. SERVICE-ONLY TIME AND MATERIAL PROCESS (WUS NOT APPLICABLE)**

The flowchart set out immediately below describes the process to be followed for the repair of Out-of-warranty devices that are not fully covered by the monthly rate. The Bidder must supply a monthly rate to co-ordinate the repair. The additional amount that will be chargeable on SARS's acceptance of the quote obtained by the Service Provider must be passed through without margin and will be chargeable in addition to the monthly rate.

**Diagram 2.1 Service Only Time and Material (out of warranty)**

3. SARS-PROVIDED WUS PROCESS

The flowchart set out immediately below describes the process to be followed for the provision of WUSs by SARS. This process must be read together with the preceding process descriptions that include the provision of WUSs.



SARS Whole Unit Spares

Diagram 3.1 SARS Provided WUS Process

4. INSTALLATION/REPLACE PROCESS

The flowchart set out immediately below describes the process to be followed for the installation of devices. This service is to be rendered as a Standard Chargeable Service

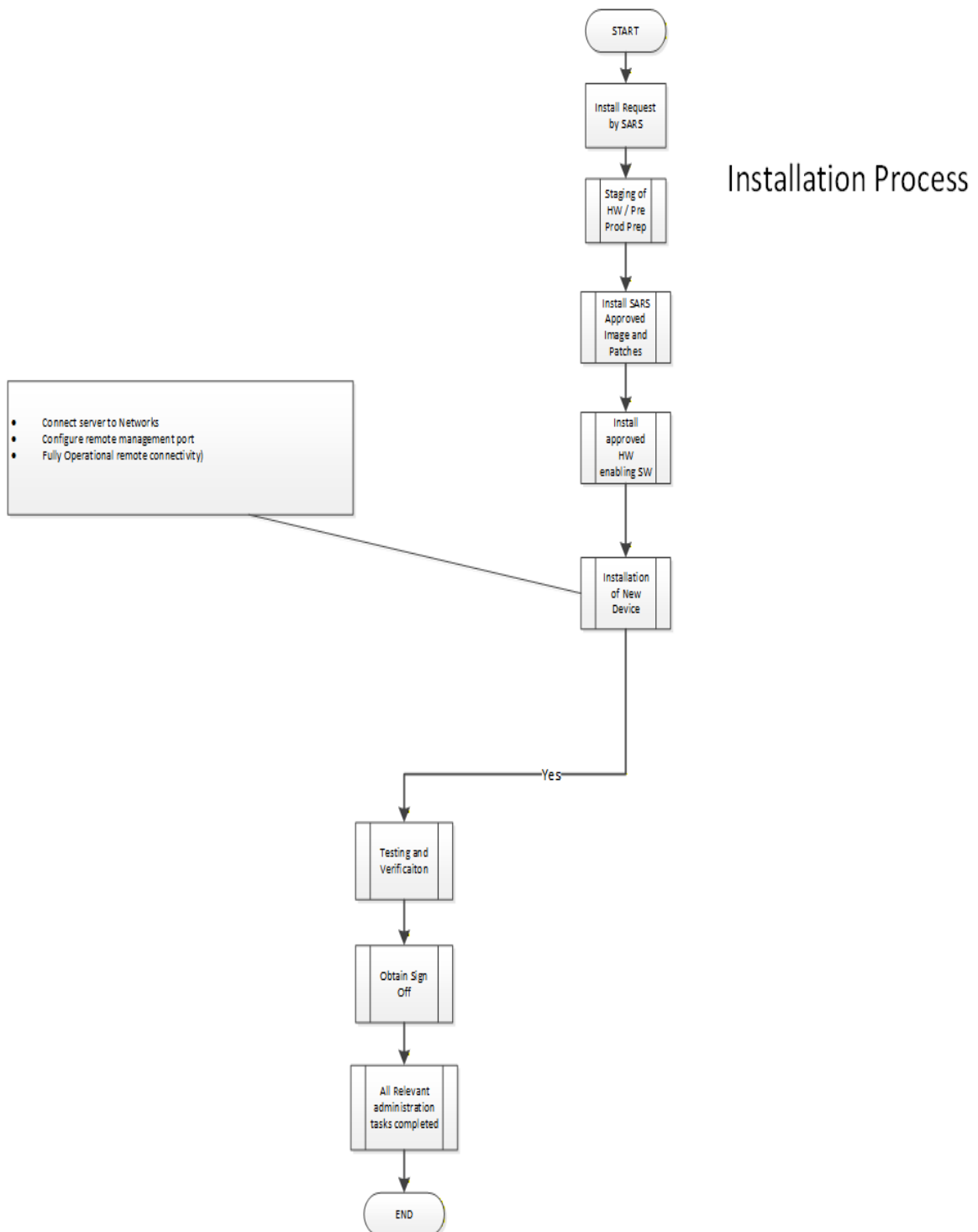


Diagram 4.1 Installation/Replacement Process

5. MOVE PROCESS

The flowchart set out immediately below describes the process to be followed for the move of devices. This service is to be rendered as a Standard Chargeable Service. Service Provider must ensure equipment is handled in line with OEM specifications whilst in transit. In the event of damage, the Service Provider will be liable.



Diagram 5.1 Move Process

6. DECOMMISSION FOR DISPOSAL

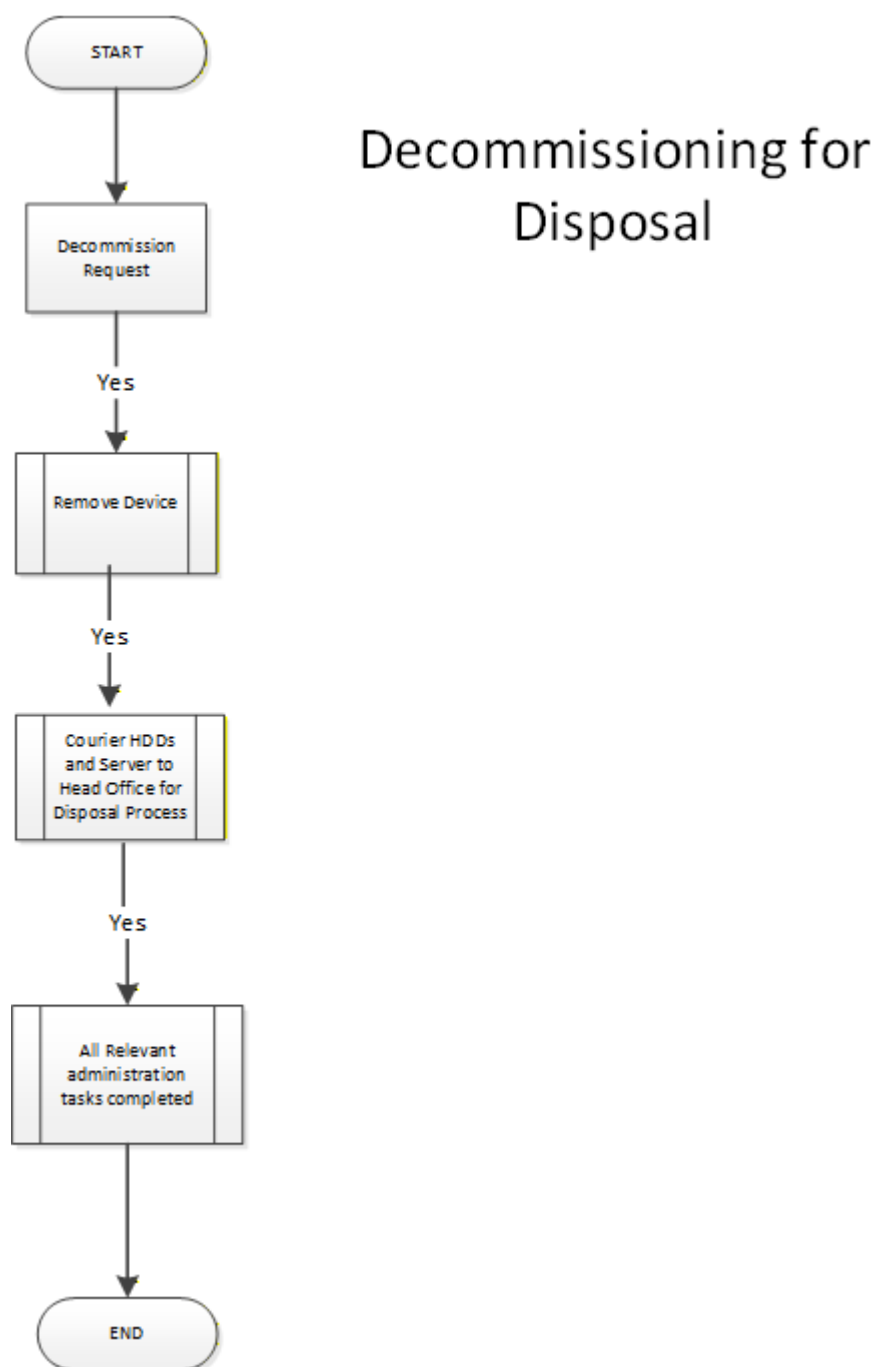


Diagram 6.1 Decommissioning for disposal

7. DELIVERY ACCEPTANCE TEST

The flowchart set out immediately below describes the process to be followed for the provision of Delivery Acceptance Test services. This service is to be rendered as a Standard Chargeable Service.

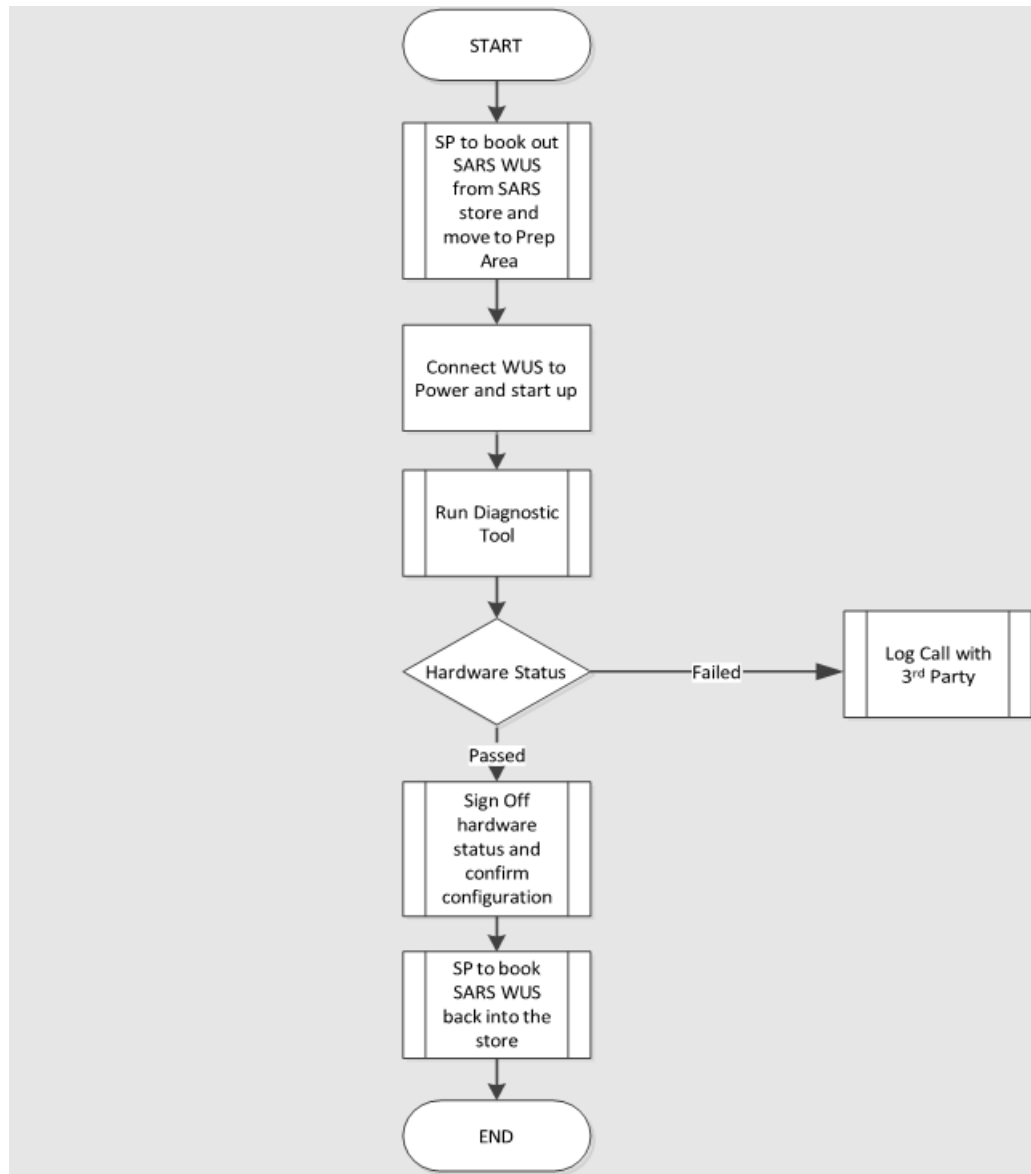


Diagram 7.1 Delivery Acceptance Test