

# **SOUTH AFRICAN REVENUE SERVICE**

## **REQUEST FOR PROPOSAL 03/2024**

### **NETWORK, SERVER AND END-USER DEVICE SUPPORT SERVICES**

#### **BUSINESS REQUIREMENTS SPECIFICATION**

## Table of Contents

1	Usage of Terms in this Document	4
2	Background	6
3	Components of Scope	7
4	Use of Alternate Technologies or Processes during the Term	7
5	Underlying Principles to the Services	7
6	Common Service Definitions and Requirements	13
7	Research and Development	28
8	Warehousing And Reverse Logistics (Tower N And Tower E Only)	31
9	Transition Process (Common Requirements)	33
10	Tower N: Network Support Services	34
11	TOWER S: Server Support Services	52
12	TOWER E: End-user Device Support Services	61
13	Award Of More Than One Tower To A Service Provider	75
	Attachment A: Process Flow Diagrams	76
1	In-warranty Break-fix process (WUS applicable)	77
2	In-warranty Break-fix process (WUS not applicable)	78
3	Out-of-warranty Break-fix process (WUS applicable)	79
4	Swap-out repair process	80
5	Service-only – Time and Material process (WUS applicable)	81
6	Service-only – Time and Material Process (WUS not applicable)	82
7	Service Provider-provided WUS Process	83
8	SARS-provided WUS Process	84
9	Pre-production Preparation/Staging Process	85
10	Installation/replace Process	86
11	Move Process	87
12	Add/Change Process	88
13	Decommissioning for Re-use Process	89
14	Decommissioning for DISPOSAL Process	90
15	REPAIR PROCESS (End-user devices)	91
16	Install Service Provider-provided Consumable Process	92
17	Install SARS-provided Consumables Process	93
18	Delivery Acceptance Test	94
19	Warehouse management Process	95
20	Reverse logistics Process	96
21	Decommissioning for Re-use Process (Networks)	97
22	Decommissioning for Re-use Process (Networks)	98

## RFP 03/2024

**Business Requirements Specification**

This document forms part of the RFP 03/2024 pack. It sets out the business requirements that SARS has for Network, Server and End-user 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;
- Network, Server and End-user Device Support Services Agreement;
- Tower N Site Classifications;
- Tower S Site Classifications;
- Tower E Site Classifications;
- Tower N Network Equipment Inventory; and
- Tower S Server Devices, and Tower E End-user Device per SARS Site.

The Network, Server and End-user Device Support Services Agreement sets out the provisions of the agreement under which SARS intends contracting with the successful Bidder(s). The Network, Server and End-user Device Support Services Agreement contains the contractual provisions for Tower N, Tower S and Tower E. The purpose of presenting the terms and conditions these Towers in a single document is to simplify the task for the Bidder in responding to the RFP as most general agreement provisions are common between the Towers. Provisions that are only applicable to one of the Towers are clearly marked in the Network, Server and End-user Device Support Services Agreement. While the Bidder is required to respond to the entire Network, Server and End-user 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), which applies to Tower N, Tower S and Tower E;
  - Schedule B-N (Network Support Services SOW), which applies only to Tower N;
  - Schedule B-S (Server Support Services SOW), which applies only to Tower S;
  - Schedule B-E (End-user Device Support Services SOW), which applies only to Tower E;
- Schedule C (Service Levels), which applies to Tower N, Tower S and Tower E;
  - Appendices C-N-1 and C-N-2, which apply only to Tower N;
  - Appendices C-S-1 and C-S-2, which apply only to Tower S; and
  - Appendices C-E-1 and C-E-2, which apply only to Tower E.

## 1 USAGE OF TERMS IN THIS DOCUMENT

### 1.1 References to other Documents in the RFP Pack

Underlined and italicised 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 capitalised terms in this document appearing in the glossary table below will have their corresponding meanings.

Term	Meaning
<b>API</b>	Application Programming Interface
<b>CSIRT</b>	Computer Security Incident Response Team
<b>CMDB</b>	Configuration Management Database
<b>Device-based Services</b>	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.
<b>End-user Device</b>	PCs, laptops, tablets, smart phones, printers, scanners and other hardware that end-users use to provide input to receive output from and generally interact with IT applications and services.
<b>Expedited Service Request</b>	See the definition in paragraph 5.12
<b>HBA</b>	Host Bus Adaptor
<b>In-warranty</b>	Refers to the status of a device that is under manufacturer warranty.
<b>KVM</b>	Keyboard, Video and Mouse
<b>OEM</b>	The original equipment manufacturer.
<b>Out-of-support</b>	Refers 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 provides any support for, the device.
<b>Out-of-warranty</b>	Refers to the status of a device that is not under manufacturer warranty.
<b>SARS PPS&amp;G</b>	SARS Policies, Procedures, Standards and Guidelines
<b>SARS Service Management System</b>	The BMC Remedy system used for the management of SARS' service management processes.
<b>SD Card</b>	Secure Digital Card
<b>SDLC</b>	System Development Lifecycle
<b>Seat</b>	Open-plan office space on a SARS site containing a desk, chair, telephone handset and network connection point. Telephone call usage costs will be recovered from the Service Provider.

Term	Meaning
<b>Server</b>	Enterprise computing platforms. The scope of this RFP includes servers based on the Intel processor family.
<b>Service Coverage Period</b>	See the definition in paragraph 5.
<b>Service Level</b>	See the definition in paragraph 5.
<b>Service-only</b>	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.
<b>Services</b>	The services to be delivered by the Service Provider as set out in clause 4 of the <i>Network, Server and End-user Device Support Services Agreement</i> .
<b>SFP</b>	Small Form-factor Pluggable.
<b>SIEM</b>	Security Information and Event Management
<b>Site Classification</b>	See definition in paragraph 5.
<b>SOW</b>	Statement of Work
<b>SOC</b>	Security Operation Centre
<b>SOAR</b>	Security Orchestration, Automation and Response
<b>SP</b>	Service Provider.
<b>Standard Chargeable Services</b>	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.
<b>Swap-out</b>	Means the activity of permanently replacing a non-functioning device with a functioning device. See paragraph 6.10.
<b>UTR or Uneconomical to Repair</b>	This term is applicable to the handling of certain repairs to out-of-warranty devices for which the Service Provider is obligated to repair for a monthly charge. See paragraph 6.8.
<b>WFH</b>	Work from Home.
<b>WUS or Whole Unit Spare</b>	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.

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

To achieve SARS's Vision 2024 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 organisational objectives.

This tender for the Tower Infrastructure contracts for Towers N, Tower S and Tower E is 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
- 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 network, server and end-user 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 network, server and end-user devices. However, during the anticipated Term of the Network, Server and End-user Device Support Services Agreement, developments in Network, Server and End-user 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 network, server and end-user devices is constantly evolving and as SARS maintains its efforts to modernise its systems, a changing mix of devices, brands and models are anticipated to be introduced during the Term of the Network, Server and End-user Device Support Services Agreement. It will, therefore, be expected of the Service Provider(s) to support a wide and evolving range of network, server and end-user devices as and when SARS may introduce them into the SARS configuration, although the award of a contract in any of the Towers does not confer the right of exclusivity to provide support services for new devices.

### 3 COMPONENTS OF SCOPE

SARS has divided the scope of the RFP into 3 (three) Towers of scope:

- Tower N:** Network Support Services;
- Tower S:** Server Support Services; and
- Tower E:** End-user Device Support Services.

### 4 USE OF ALTERNATE TECHNOLOGIES OR PROCESSES DURING THE TERM

In defining the scope of the Towers, 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 all 3 (three) Towers (Tower N, Tower S and Tower E).

#### 5.1 Accountability

SARS requires a single, accountable Service Provider for the Services to be delivered in each Tower. SARS does not necessarily require the Service Provider in a Tower to provide all the Services itself. The Service Provider may source different elements of the services from other service providers provided that the Service Provider manages the provision of the individual elements in a seamless manner from SARS's perspective and takes full accountability for the Services meeting the required contractual performance standards. 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 in a Tower 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-exclusivity

SARS intends to contract for the different areas of scope within a Tower with a 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 in any Tower 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 in any of the Towers. If SARS undertakes a transformation of technology or process within the scope of a Tower during the Term, the Service Provider appointed to such Tower 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.



SARS is currently undertaking LAN transformations towards branches (15) from Cisco Catalyst to Cisco Meraki that should be completed by June 2024.

## 5.5 Compliance

The Service Provider is required to execute the processes, procedures, schedules and work practices developed in accordance with the Network, Server and End-user 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 Network, Server and End-user 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 Network, Server and End-user 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 Network, Server and End-user Device Support Services Agreement.

The Bidder's attention is drawn to the Service Level Targets and the provisions of Schedule C of the Network, Server and End-user 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 (per Tower N, Tower S and Tower E) 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 WFH, 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 or Platinum) which describes the repair time applicable to a 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 device-based service for every combination of Site Classification (Metro, Town or Rural); Service Coverage Period (WFH, Basic, Standard, Extended and Premium) and Service Level (Bronze, Silver, Gold or Platinum) for every device type.

The definitions of Bronze, Silver, Gold or Platinum within each of Tower N, Tower S and Tower E; and the definitions of WFH, Basic, Standard, Extended and Premium within each of Tower N, Tower S and Tower E 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 Device**

In each Tower, each SARS Site has been assigned a Service Level and Service Coverage Period that applies to all devices in the Tower that are registered to that SARS Site. The Service Level and Service Coverage Period assigned to a SARS Site may differ between the Towers. At the Commencement Date, the Service Level and Service Coverage Period assigned to a site for a Tower will be as specified in *SARS Site Classifications (per Tower N, Tower S and Tower E)*. 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 mobile device (such as a laptop), which has been moved from the site at which it is registered, then the Service Provider must still provide support for the 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 laptop registered at Beit Bridge has a Service Coverage Period of “Standard” and a Service Level of “Silver”. The laptop 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 (per Tower N, Tower S and Tower E) 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 Special conditions relating to WFH Service Coverage Period

The WFH Service Coverage Period will only apply in Tower E and may not be assigned to a SARS device in Tower N not Tower S. The WFH Service Coverage Period in Tower E may only be assigned to a SARS owned or rental device used by a SARS end-user classified as a WFH user.

SARS may not assign a WFH Service Coverage Period to a SARS device unless SARS has completed the necessary verifications that the end-user in question is in fact a WFH user.

#### 5.11 Measurement and Reporting of Service Levels

The Service Provider must produce monthly Service Level reports in accordance with Schedule C of the Network, Server and End-user Device 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.

## 5.12 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 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.

## 5.13 OEM Relationship

The Service Provider must have a back-to-back agreement in place with the applicable OEMs (or their official representatives) 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 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 *Network, Server and End-user Device 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 *Network, Server and End-user 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 with OEMs (or their official representatives) to accommodate SARS's requirement for support for the newly introduced equipment/brands.

## 6 COMMON SERVICE DEFINITIONS AND REQUIREMENTS

Regardless of the Tower(s) in which a Service Provider has been appointed, it must provide all the services detailed in this paragraph 6 unless otherwise specified.

### 6.1 Service Management

The Service Providers appointed in each of the Towers 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 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 ticket, 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 licences, it will be at the Service Provider's cost.

The Service Provider may, in addition and 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 licences that SARS will make available to the Service Provider for Tower N, Tower S and Tower E, respectively. The Service Provider may, during the Term, with 30 (thirty) days' notice, request additional Service Management licences. However, the Service Provider must note that the costs associated with such additional licences will be recovered from the it.

**Table C-1. SARS Service Management System licences that will be made available per Service Management module for Tower N, Tower S and Tower E, respectively**

License type	Tower N	Tower S	Tower E
Change Management	1 X Service Management Suite Named	1 X Service Management Suite Named	2 X Service Management Suite Named
Configuration Management	1 X Service Management Suite Named	1 X Service Management Suite Named	5 X Service Management Suite Named
Incident Management	2 x Service Desk Named	2 x Service Desk Named	6 x Service Desk Named
Problem Management	1 x Service Desk Named	1 x Service Desk Named	1 x Service Desk Named
Release Management	1 x Service Desk Named	1 x Service Desk Named	1 x Service Desk Named

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

The table below sets out the number of Seats that SARS will make available for Service Provider personnel performing service management services for Tower N, Tower S and Tower E, respectively.

**Table C-2. Number of Seats provided by SARS for use by Service Provider service management personnel**

Function	Site	Tower N	Tower S	Tower E
Change Management	Lehae La SARS	0	0	0
Configuration Management	Lehae La SARS	0	0	0
Incident/Problem Management	Lehae La SARS	0	0	0
Incident Co-ordinator	Lehae La SARS	1	0	0
Release Co-ordinator	Lehae La SARS	0	0	0

The Service Provider must ensure that sufficient personnel is 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 licences and Seats and must submit a request to SARS for the increase/decrease of the number of licences and/or Seats 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 licences and Seats that are requested by the Service Provider in excess of the numbers in Tables C-1 and C-2. SARS will, on a regular basis, review the licence and Seat utilisation across all services and functions by the Service Provider and if the number of licences and Seats provided by SARS cannot be justified, SARS reserves the right to reduce the allocations accordingly.

## 6.2 Device-based Services

The applicability of these Device-based Services to the categories of Tower N Network Devices is set out in paragraph 10.

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

The applicability of the Device-based Services to categories of Tower E End-user Devices is set out in paragraph 12.

## 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 Network, Server and End-user Device Support Services Agreement, in particular Schedule B (Service Management Services SOW); Schedule B-N (Network Support Services SOW); Schedule B-S (Server Support Services SOW); and Schedule B-E (End-user Device 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-N (Network Support Services SOW); Schedule B-S (Server Support Services SOW); and Schedule B-E (End-user Device Support Services SOW) of the Network, Server and End-user 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 device;



- Specifying any visible damage or defect to the 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 device;
- Verifying the asset information (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 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 device are functional and operating before the call is closed;
- Verifying that the user/owner information is correct;
- 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(s) across all the Towers. The Break-fix services that are required for the device categories in each of the Towers are listed in Table N-2 for Tower N, Table S-2 for Tower S and Table E-2 for Tower E. 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 Swap-out services and Break-fix In-warranty services for network devices. SARS may elect to receive Break-fix In-warranty services for router equipment that is still under warranty and for Out-of-support router equipment, SARS may elect to receive Swap-out services. SARS will

pay the monthly per device Break-fix In-warranty fee for its routers that are under warranty and the monthly per device Swap-out services fee for its Out-of-support routers and receive the services accordingly.

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 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 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 contract with a third-party provider 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 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 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 devices, the Bidder must provide full Break-fix services, including the repair for the monthly rate. The Bidder must, therefore, include the cost of all activities, parts, labour, etc. to effect repair of the device in the monthly rates.

If the cost to repair an Out-of-warranty 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 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 Devices that Require only the Facilitation of Repair (Exclude actual repair activities)**

For this category of 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 device. These devices will be categorised as “**Service-only**” devices.

The Service Provider must engage a certified repair provider(s) for the repair of the 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 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 mark up. 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 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 devices (“**Swap-out**” devices), the Service Provider must permanently replace faulty 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 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 device and the faulty device. The faulty 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 device must be a SARS asset. The Swap-out service is not to be confused with the WUS service, which *temporarily* replaces a faulty device with a functioning device while the faulty 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 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 applicable	Attachment A Diagram 1
In-warranty where a WUS is not applicable	Attachment A Diagram 2
Out-of-warranty where a WUS is applicable	Attachment A Diagram 3
Swap-out repair	Attachment A Diagram 4
Service-only repair where a WUS is applicable	Attachment A Diagram 5
Service-only repair where a WUS is not applicable	Attachment A Diagram 6
Service Provider-provided WUS process	Attachment A Diagram 7
SARS-provided WUS process	Attachment A Diagram 8

### 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 of 20, 50 and 100 for Tower E, and 5, 10 and 15 for Tower N 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 devices will be less than the aggregate of the Standard Chargeable Service charges if SARS was to request them individually per 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 devices.

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	
Pre-production Preparation/Staging	Attachment A Diagram 9 The Service Provider may be expected to attach a SARS barcode as part of the Pre-production Preparation/Staging process.
Installation	Attachment A Diagram 10
Replace	Attachment A Diagram 11 (The replace process is included in the process flow for Installation)
Move	Attachment A Diagram 12 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.
Add/Change	Attachment A Diagram 12.1
Decommission for Re-use	Attachment A Diagram 13.1
Decommission for Disposal	Attachment A Diagram 22.1
Repair/Support	Attachment A Diagram 15.1

Expedited Service Request	<p>On request by SARS:</p> <ul style="list-style-type: none"> <li>• Provide SARS with a commitment to the best possible time to respond/repair a device.</li> <li>• On acceptance of the expedited commitment, perform accordingly.</li> <li>• Obtain signoff from a SARS representative.</li> <li>• Submit invoice for Expedited Service Request.</li> </ul> <p>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.</p> <p>(No process flow diagram is presented for Expedited Service Requests)</p>
Consumable (Service Provider-provided)	Attachment A Diagram 16
Consumable (SARS-provided)	Attachment A Diagram 17
Delivery Acceptance Test	<p>Attachment A Diagram 17</p> <p>The Service Provider may be expected to attach a SARS barcode as part of the Delivery Acceptance process.</p>

#### 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	<p>On request by SARS:</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• On acceptance of the quotation by SARS, perform the courier service.</li> <li>• Invoice SARS as per the proposal, either on the completion of milestones or otherwise as agreed in the proposal.</li> </ul> <p>Service Provider to update the CMDB.</p> <p>Asset Management</p>

## 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	
	<p>Identity Verification: The Bidder should ensure that verification of recipient's Identity is done to ensure they are delivering items to the correct person.</p> <p>Physical Security: The Bidder should ensure that the equipment can be transported with armed security for large shipments between sites on request.</p> <p>Integration with Warehouse Services</p> <p>The Bidder should ensure that their transport services are integrated into their warehousing solution</p>
Project Service	<p>On request by SARS:</p> <ul style="list-style-type: none"> <li>• Provide a quotation for Project Services</li> <li>• On acceptance of the quotation by SARS, perform the project service.</li> <li>• Invoice SARS as per the proposal, either on the completion of milestones or otherwise as agreed in the proposal.</li> </ul> <p>Service Provider to update the CMDB.</p>
Warehousing	<p>On request by SARS:</p> <ul style="list-style-type: none"> <li>• Provide a quotation for the secure storage of devices.</li> <li>• On acceptance of the quotation by SARS, perform the storage service.</li> <li>• Invoice SARS as per the proposal, either on the completion of milestones or otherwise as agreed in the proposal.</li> </ul> <p>Service Provider to update the CMDB.</p>

For clarity, the table below sets out the responsibilities of certain services applicable to Tower N, Tower S and Tower E 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.

Responsibilities related to services which are only applicable to Tower N are set out in paragraph 10.5.



**Table C-6 High level division of responsibilities common to Tower N, Tower S and Tower E**

Scope		Responsibilities	
		Service Provider	SARS
Device-based Services	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 device within the scope of services, route to Service Provider.
	Receive ticket.	Service Provider must receive the ticket from the SARS system.	
	Perform onsite diagnosis and repair/Swap-out	Service Provider must confirm 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.	
	Secure Storage Space	On request by SARS: provide quote at standard rates; on acceptance, provide storage space	
	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. At least one of the Service Delivery Manager and 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 *Network, Server and End-user 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 N and Tower S, the Service Delivery Manager and Operations Manager will be one person with multiple roles. The Account Executive in all Towers will be non-billable as this is a standard practice for Service Delivery. Operations Manager should not be deployed to perform technical functions.

The table below sets out the number of Seats that SARS will make available for Service Provider onsite management personnel for Tower N, Tower S and Tower E, respectively.

**Table C-7 Number of Seats provided by SARS for use by onsite management personnel**

Function	Site	Tower N	Tower S	Tower E
Account Executive/Service Delivery Manager	Lehae La SARS	0	0	1
Operational Manager	Lehae La SARS	1	1	1

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 Network, Server and End-user 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 x Pricing Response Template (where x is the applicable Tower reference).

#### 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 Network, Server and End-user 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 Network, Server and End-user 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 optimise 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 in the areas listed below.

### 7.1 Tower E: End-user Device Support Services

Service Providers should monitor and analyse trends, emerging technologies, and best practices in the field of end-user devices, taking into consideration device compatibility, functionality, and security. The Service Provider should provide strategic guidance on device selection, innovative approaches to device management, and advanced troubleshooting and diagnostic tools to ensure seamless user experience, productivity, and cost-effectiveness.

### 7.2 Tower E: Research and Development Initiative

SARS is currently in the standardisation process of selecting two standard brands from among several leading Multi-Function Printer (MFP) manufacturers, including Brother, Canon, Epson, Fujifilm, HP, Konica Minolta, Kyocera, Lexmark, Ricoh, Sharp, Toshiba, and Xerox. This decision, aimed at streamlining our MFP infrastructure for enhanced operational efficiency and support simplicity, will be finalised during or shortly before the contract commencement with the chosen service provider for Tower E RFP 03/2024.

Service Providers must show that they are prepared to support whichever two brands SARS ultimately selects. This includes having the necessary OEM accreditation to provide comprehensive support for these brands, ensuring that the Service Provider's team is ready to offer proficient hardware and parts assistance immediately upon brand selection. The successful Bidder will be expected to quickly ensure that their staff are fully trained and up to date with the necessary skills to support the chosen MFP brands, 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 the selected MFP brands, ensuring swift and effective responses to service requests. This also involves proactive engagement with the OEMs to stay abreast of technological updates, ensuring that SARS benefits from high-quality, secure MFP solutions. This approach aims to uphold a robust, efficient MFP environment tailored to meet SARS's specific operational requirements and security protocols.

### **7.3 Tower S: Severs Support Services**

Service Providers should conduct research and development activities focused on server technologies, including hardware, virtualisation, and cloud solutions. They should assess the performance, scalability, and security of the current server infrastructure and recommend enhancements and upgrades to align with SARS's evolving needs and strategic objectives. This includes exploring energy-efficient and sustainable solutions to minimise environmental impact.

#### **7.3.1 As part of Device-based research and development Services in Tower S, the Service Provider must:**

- a. Ensure that the server device operating systems are supported, and all OEM-recommended firmware are installed in line with SARS PPS&G;
- b. Inform SARS of any announcements made by the device OEM regarding hardware and software end of support dates; and
- c. Follow the SARS service management procedures to ensure that the servers are maintained in accordance with the SARS PPS&G.

SARS may request for 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 as 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.

#### 7.4 **Tower N: Network Support Services**

Service Providers should investigate advancements in network support services, including but not limited to, routers, switches, firewalls, and wireless access points. The focus should be on improving network performance, reliability, and security, in addition to evaluating new technologies and protocols that can enhance the overall network architecture.

The research and development services outlined are integral to the continuous improvement and success of the Service Provider's offerings. Bidders must display a strong commitment to research, development and innovation, ensuring that they are consistently meeting and exceeding the expectations of SARS in the areas of end-user device support, server support, and network support services.

#### 7.5 **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.

##### 7.5.1 **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.

##### 7.5.2 **Proactive Technology Support**

The Service Provider shall proactively monitor and stay informed about advancements in technology and industry best practises 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.

##### 7.5.3 **Scalable Support Model**

The Service Provider shall implement a scalable support model capable of accommodating the growth and expansion 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.

#### 7.5.4 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.

#### 7.5.5 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.

### 8 WAREHOUSING AND REVERSE LOGISTICS (TOWER N AND TOWER E ONLY)

Warehousing (Storage Facilities) is required for Tower N and Tower E (not Tower S) in the following regions throughout South Africa:

- Gauteng (Pretoria);
- Mpumalanga (Nelspruit);
- KwaZulu-Natal (Durban Metro);
- Eastern Cape (East London);
- Eastern Cape (Gqeberha);
- Western Cape (Cape Town);
- Northern Cape (Upington);
- Limpopo (Polokwane);
- Northwest (Potchefstroom); and
- Free State (Bloemfontein).

The Warehousing services must comply with general accepted safety and security standards as noted in ISO 9001, ISO 14001, ISO 45001 and ISO 27001 and always align to industry best practices during the term of the contract. Paragraph 8.1 fully describes functionality required of Warehousing services/management.

As SARS strives for efficiency and cost-effectiveness, the process of reverse logistics plays an increasingly important role in device management. A Service Provider with geographically dispersed warehousing capabilities will offer seamless solutions for handling device distributions, returns and redistributions. This approach not only exemplifies environmental responsibility, but also assists in maintaining a clutter-free workplace by ensuring that only operational computers are present on SARS's premises. Consequently, the Service Provider's reverse logistics capabilities ensure a streamlined process for device lifecycle management, while promoting physical endpoint security and asset management best practices.



New endpoints should be configured on SARS premises to SARS standards and subsequently booked into the Service Provider's reverse logistics system. From that point, devices should be efficiently handed over to users at a branch location, or potentially, in the future, delivered directly to the user's home.

In line with technological advancements and evolving industry standards, the configuration of the devices will continuously mature and modernize over time. As new automation capabilities become available, the Service Provider will ensure seamless integration of these features, enhancing both performance and user experience. This progressive approach not only enables SARS to stay ahead in the rapidly changing digital landscape, but also ensures that their device lifecycle management remains efficient and cost-effective. Moreover, adopting modern configurations will empower SARS to maintain its focus on security and sustainability while promoting innovation and adaptability within its workforce.

Outdated, replaced devices will be collected from end users and entered on the reverse logistics system for assessment. During this stage, they will be evaluated for possible refurbishment and potential re-issuing to other users. If refurbishment is deemed unfeasible, the devices will be decommissioned in accordance with SARS's regulations and best practices. This systematic approach ensures that SARS's resources are optimised, contributing to a more sustainable and cost-effective device lifecycle management process.

The decommissioning and disposal process for devices that are no longer suitable for use within SARS will be performed according to SARS's internal policies and operating procedures, which may include redeployment, donations, sale, and destruction.

The Service Provider must also have the necessary facilities, resources, and expertise to perform diagnostic assessments, repairs, and refurbishments of end-user devices as required. This includes maintaining a supply of spare parts and components to minimise repair turnaround times and maximise device uptime.

## 8.1 Warehouse Management Portal

The Service Provider must have implemented the planned Warehouse Management Portal as accepted and approved by SARS before the end of the Transition project. Any changes identified in the Transition project must be fully operational within the Warehouse Management Portal within 90 (ninety) days thereafter.

The Service Provider must provide a Warehouse Management Portal that delivers, at a minimum, the following functionality to SARS through a secure internet connection:

- **Inventory Management:** The platform must provide comprehensive inventory management features, including tracking device quantities, locations, and statuses (e.g., stored, donated, or sold). The system must enable real-time updates, alerts for high and/or low stock levels, audit trails, and reporting tools for inventory analysis.
- **Reporting and Analytics:** The Warehouse Portal must include reporting and analytics capabilities, offering insights into inventory levels, and other relevant



data. These insights can inform decision-making, optimise warehouse utilisation, and identify areas for improvement.

- **User Management and Access Control:** The system must provide robust user management and access control features, ensuring that only authorised staff members can access and interact with the Warehouse Portal. This includes options for role-based permissions, secure authentication methods, and audit logging for tracking user activity.
- **Scalability and Flexibility:** The Warehouse Portal must be designed to scale and adapt to SARS's changing needs, accommodating growth in the number and variety of devices managed and the evolving requirements of the reverse logistics and warehousing processes.

The Bidder is required to provide details of its current capability to deliver the Warehouse Management Portal requirements as set out above, as well as details of its plan, including timelines to which the Bidder is prepared to commit, to implement the full functionality as set out above. SARS's requirement is to have the Warehouse Management Portal fully operational 3 (three) months after the Commencement Date.

The Bidder shall be responsible for the development and implementation of a comprehensive Warehouse Portal solution in compliance with the requirements outlined herein, adhering to industry best practices for user experience, security, and performance.

Furthermore, the Bidder shall maintain open channels of communication and engage in continuous collaboration with SARS to ensure the Warehouse Management Portal aligns with SARS's needs and expectations and adapts to evolving requirements. The Bidder is obligated to deliver a Warehouse Portal solution that meets the stipulated requirements and integrates effectively with the existing systems, thereby enabling the efficient management of end-user devices within SARS.

## 9 TRANSITION PROCESS (COMMON REQUIREMENTS)

NB: The following requirements are common across the Towers. For transition timelines, refer to the relevant section for each Tower.

### 9.1 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 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 NSE 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.

## 9.2 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/Programme Management, Vendor and Contract Management, IT Service Management and Technical Subject matter experts.

# 10 TOWER N: NETWORK SUPPORT SERVICES

## 10.1 Scope

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

- Network support services (Device-based Services, Standard Chargeable Services, project, consulting, training) for SARS-owned and SARS-managed network infrastructure, including hardware and software support for Routers, Switches, Gateways, Firewalls, Load Balancing Equipment (F5), CISCO Unified Communication Managers.
- Administration, maintenance of Cisco ACI Network Infrastructure at the SARS Hosting Site at Vodacom, Brooklyn Lehae La SARS, Alberton Campus and Doringkloof — centralised from Brooklyn.

- Administration of Network Management Systems (CISCO DNA Centre, CISCO Prime Infrastructure), centralised from Brooklyn.
  - The CISCO DNA and PI high-level infrastructure consists of the following components:
    - 2 \* CISCO PI Virtual Appliances
    - 1 \* CISCO DNAC Appliance
- Administration services for SARS's CISCO Unified Communication Managers centralised from Brooklyn. The context of services required is captured in the Network SOW:
  - The CISCO Unified Communication Managers high-level infrastructure consists of the following components:
    - 1 \* CISCO Call Manager Publisher (IOS ver 12.5)
    - 5 \* CISCO Call Manager Subscriber (IOS ver 12.5)
    - 1 \* CISCO IM & Prescence Server (IOS ver 8.10)
    - 8 \* CISCO ASR 1001 Routers (IOS ver 16.0)
    - Licences

CUWL	10
Enhanced Plus	108
Enhanced	5 998
Basic	1 219
Essential	1 871
Telepresence	23

- Supply and installation of network equipment and software for resolution of break-fix incidents.
- Supply of maintenance and Break-fix service for patch- and server rooms (cleaning, painting, lightning and provision of power points/PDUs within cabinets).
- Supply and installation of network points, cabling and associated cabling equipment for example but not limited to high-band frames, termination blocks, patch panels and brush panels.
- Network security services (software licensing, maintenance and support services) will be required during the Term for firewall, network admission control and remote access services (including client-side software and maintenance, appliances and software tokens).
- Administration of Digital Signage (PADS4), centralised from Brooklyn. Management, support and maintenance, including software and additional PADS4 licencing. The PADS4 infrastructure consists of the following components:
  - 4 PADS4 Servers, 2 sets of Primary and Backup Servers (internal and external (DMZ) facing);
  - 100 PADS4 HTML SOC Screens;
  - 150 PADS4 Expert Agents (Branch Kiosks, Windows-based); and

- 25 PADS4 Full Viewers (Contact Centre Dashboards, Windows-based).
- Management of OEM and Third-party support contracts.
- Fraud and Phishing Detection Services (an anti-phishing service).
- Provision of application security assessments, penetration testing and vulnerability assessments.
- Symantec Endpoint Protection and Symantec Data Loss Prevention, management, support and maintenance. May only be required from 1 October 2026 at SARS's sole discretion.
- CISCO NAC management, support and maintenance.
- Managed SOC Services, with full integration to the SARS QRadar SIEM.
- The common services set out in paragraph 6, including service management, Service Provider management personnel, administration, consulting, project management and support.

The services, at a high level, comprise the management of incidents, the provision of defined services relating to the supported equipment, maintenance services; supply of consumables; professional services; the provision of Standard Chargeable Services such as install, move, add, change and decommissioning services; and compliance with required service management procedures. The required services include Cisco Professional Services, to provide for the escalation of Cisco hardware and software related incidents and configuration related incidents.

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

- a. Ensure that the network device operating systems are supported, and all OEM-recommended patches/firmware are installed in line with SARS PPS&G;
- b. Inform SARS of any announcement made by the device OEM regarding hardware and software end of support dates;
- c. Follow the SARS service management procedures to ensure that the software is maintained in accordance with the SARS PPS&G; and
- d. Resolve operating system software incidents as part of the Break-fix services.

During the Term, SARS may request quotations and procure network devices and related software to resolve break-fix incidents, for example, to replace a malfunctioning device that is UTR. The inclusion of the procurement of network devices for the resolution of Break-fix incidents in the scope of this RFP is non-exclusive and SARS may procure network devices from other parties during the Term.

## 10.2 Delivery Model

The SARS Bridge (NOC) is responsible for Network Monitoring, including “Carrier Management”, and the Service Provider appointed will be expected to integrate with the provision of these services as required by The SARS Bridge (NOC). SARS’s requirements for network services are now limited to the scope as described in paragraph 10 which covers the support and configuration of the network, excluding the aspects of network management, carrier management and network monitoring.

Network design, monitoring, capacity and performance management may be requested by SARS on a time and material basis in the delivery model.

## 10.3 Transition

The Service Provider appointed in Tower N is required to complete the Transition Services within 3 (three) months from the Effective Date. By the end of the 3 (three) months, the Service Provider must have assumed full management responsibility for the full scope of Network Support Services. In addition to any other commitment required in the Network, Server and End-user 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 Network, Server and End-user Device Support Services Agreement, especially those detailed in Schedule B-N and its attachments;
- Audited and verified the status of all Network Devices within the current Storage Facilities and transferred them to the Service Providers Storage Facilities as set out in Schedule C and Appendices C-N-1 and C-N-2 of the Network, Server and End-user 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;
- Established the required governance as specified in Schedule E of the Network, Server and End-user Device Support Services Agreement;
- Taken over the management of any network support services that are sourced through third parties;
- Ensured that personnel assigned to the SARS account will be in possession of the minimum qualifications and experience when dealing with the corresponding technologies / services as per paragraph 6.12; 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 billing. If an incident is logged for a

device that is not recorded on SARS's CMDB but that falls into the categories of supported network 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 such 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 Network, Server and End-user Device Support Services 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. If 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.

#### 10.4 **Device-based Services applicable to Tower N**

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

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

- Tower N Site Classifications; and
- Tower N Network Equipment Inventory.

One of the objectives in this RFP is to achieve flexibility in the procurement of services. In this regard, Table N-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 network 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 N Pricing Response Template for the details of the rates that must be supplied by the Bidder.

During contract finalisation, SARS will make an election for 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 CISCO 2821 routers. SARS may elect during contract finalisation to contract for Break-fix services (In-warranty) and Break-fix services (Out-of-warranty). With 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 N-1: Categories and types of Network Equipment

Category and Types
<b>WAN Network Equipment</b>
CISCO Router 2951
CISCO Meraki Security Appliance (MX68CW)
<b>LAN Network Equipment</b>
CISCO Catalyst 3650C 8-Port
CISCO Catalyst 3650 24-Port
CISCO Catalyst 3750 24-Port (V1 and 2)
CISCO Catalyst 3750G 12-Port (SFP Based)
CISCO Catalyst 3850 24-Port
CISCO Catalyst 3750 48-Port
CISCO Catalyst 3750G 24-Port
CISCO Catalyst 3750X 24-Port
CISCO Fabric Extender N2K-C2232PP
CISCO Fabric Extender N2K-C2232TM-10GE
CISCO Meraki Camera (MV32, MV52)
CISCO Meraki Switches (MS120-8P + 24P, MS250, MS350)
CISCO Meraki Access Points (MV36)
CISCO Meraki Sensors (MT10, MT20, MT30)
CISCO Meraki Cellular Gateway (M41E)
CISCO Firewall ASA5550
CISCO Firewall ASA5555
Blade Server Chassis Switches
F5 Load Balancers (i7800, i5800)
<b>Wireless Network Equipment</b>
CISCO 2504 Series Wireless Controller
CISCO 5508 Series Wireless Controller
CISCO 9200 Series Wireless Controller
<b>Video Conferencing Equipment</b>
CISCO Spark Kit-Plus
<b>Voice Equipment</b>
CISCO UCS
CISCO ASR 1000 (SIP Gateway)
Radisys Media Server
Plantronic Headsets
<b>Network Software</b>
CISCO Prime Infrastructure
CISCO ISE
CISCO DNA Center
RSA SecurID
PADS4 Digital Signage
<b>Network Kiosks</b>
ATM (Purpose Build)
Windows Kiosks



**Table N-2: Detailed Description of Device-based Break-fix Services Applicable to Network Equipment Categories**

Category	Break-fix Services				Notes
	In-warranty	Out-of-warranty	Swap-out	Service-only	
Network Computing Devices					
WAN Network Equipment	SP-provide d WUS	SP-provided WUS	SARS-provided Swap-out device	No WUS applicable	<p>The Service Provider must provide a WUS to meet the Service Levels on devices that are not Out-of-support.</p> <p>The Service Provider must use SARS-provided Swap-out devices for Out-of-support devices.</p>
LAN Network Equipment	SP-provide d WUS	SP-provided WUS	SARS-provided Swap-out device	No WUS applicable	<p>The Service Provider must provide a WUS to meet the Service Levels on devices that are not Out-of-support.</p> <p>The Service Provider must use SARS-provided Swap-out devices for Out-of-support devices.</p>
Wireless Network Equipment	SP-provide d WUS	SP-provided WUS	SARS-provided Swap-out device	No WUS applicable	<p>The Service Provider must provide a WUS to meet the Service Levels on devices that are not Out-of-support.</p> <p>The Service Provider must use SARS-provided Swap-out devices for Out-of-support devices.</p>
Video Conferenci ng Equipment	SP-provide d WUS	SP-provided WUS	SARS-provided Swap-out device	No WUS applicable	<p>The Service Provider must provide a WUS to meet the Service Levels on devices that are not Out-of-support.</p> <p>The Service Provider must use SARS-provided Swap-out devices for Out-of-support devices.</p>
Voice Equipment	SP-provide d WUS	SP-provided WUS	SARS-provided Swap-out device	No WUS applicable	<p>The Service Provider must provide a WUS to meet the Service Levels on devices that are not Out-of-support.</p> <p>The Service Provider must use SARS-provided Swap-out devices for Out-of-support devices.</p>
Network Managem ent Software	N/A	N/A	N/A	No WUS applicable	<p>The Service Provider must maintain the currency of software maintenance and support the software in the event of incidents.</p>



## 10.5 Network Support Services Scope and Responsibilities Summary

SARS has summarised the scope and responsibility for services common to all Towers in paragraph 9.4 above. The scope and responsibility of services specific related to Tower N is set out in Table N-3 below. For Tower N the Service Provider must refer to both the table in paragraph 9.4 and Table N-3.

For clarity, Table N-3 below sets out the responsibilities of certain services applicable only to Tower N with the high-level responsibilities expected of the Service Provider and the basis on which the Service Provider is engaged. The purpose of Table N-3 is to provide clarity to the boundaries of scope and does not set out to describe the full scope of Tower N.

**Table N-3: High level division of responsibilities in Tower N**

Scope		Responsibilities	
		Service Provider	SARS
	<b>Cabling</b>	On request by SARS, provide quote at standard rates; on acceptance, perform cabling.	Initiate request
	<b>Patch/Network Room Maintenance</b>	On request by SARS, provide quote at approved rates; on acceptance, perform maintenance.	Initiate request
	<b>Fraud and Phishing Detection Services</b>	On request by SARS, implement and provide services.	Initiate request
	<b>Warehousing Facilities</b>	During Transition provide quote for Storage Facilities at locations as per paragraph 6.14.	Transition
	<b>Billing</b>	During Transition ensure that MSA Billing and invoicing requirements are documented and signed-off.	Monthly
	<b>VPN Remote Access Services (RAS)</b>	Provide hardware and software maintenance and support services. On request by SARS provide professional services.	Initiate request

## 10.6 Fraud and Phishing Detection Services

The Bidder must propose a solution, which may include the services of a subcontractor, which incorporates a comprehensive set of measures to ensure end-to-end protection against the threats of phishing attacks, which must include proactive monitoring, as well as automated and manual take-down solutions.

The solution must proactively track occurrences of SARS's names, brands, trademarks and slogans on the Internet. The solution must identify sites that may be

trying to perpetuate fraud, conduct phishing attacks, attempt identity theft by impersonation, or are fraudulently purporting to have a relationship to SARS.

#### **10.6.1 Proactive Monitoring**

Fraud detection services. This element of the service must automatically identify possible fraud on the Internet that involves SARS's name. The services must, at a minimum, include the following:

- Daily DNS searches;
- Front page searches;
- SSL site searches;
- App Store Searches: search official and unofficial stores for apps that impersonate legitimate SARS applications;
- Social Media Searches: search for specific patterns to find fraudulent Facebook, X, Instagram and other social media accounts;
- Search Engine Advertising Searches: search sites including Google, Bing, Yahoo, DuckDuckGo, automatically classifying and monitoring the resulting websites to detect fraudulent sites;
- DMARC Forensic Report Processing: analyse the status of all your SARS domains, report any configuration changes required, and highlight unprotected domains being used by fraudsters; and
- Brand infringement, including survey scams.

#### **10.6.2 Take-down Services**

On detection of possible fraud on the Internet involving SARS's name, the Service Provider must investigate and on confirmation of risk initiate a request to the relevant ISP to take down the offending site. SARS's requirement is that at least 80% of detected and confirmed risk sites be taken down within 24 hours of being confirmed and the remainder must follow a manual process to conclusion.

The Service Provider must provide SARS with a monthly report of validated SARS phishing attacks detected, detailed take-down statistics and a breakdown of actions taken. The reports to SARS should include take-down progress tracking and phishing attack monitoring.

Should an offending site not be taken down by an ISP within a reasonable period after the request to the ISP, the Fraud and Phishing Detection service proposed must include the services of specialists who must investigate the website to identify additional contacts that might be able to assist with the take-down and contact them until they have accomplished the take down.

The service proposed must include unlimited automated take downs per year and, in cases where phishing sites cannot be taken down using the automated process, the service must include a manual process. Provision must be made for 100 manual takedowns per year. The service proposed must include monitoring of every take-down process for a period of 7 (seven) days after the take down. If the site returns within the 7 (seven) days, the Service Provider must restart the take-down process. The unsuccessful take down of a site during this period will not count towards the manual take-down annual limit.

SARS may increase the take-down annual limit during the Term and the pricing structure for additional take downs must be given.

## 10.7 VPN Services

The Service Provider is required to take on and provide ongoing software maintenance for the client software and tokens as listed below, as well as the provide additional software licences. For clarity, the requirement is not for the operation of the service.

The SARS VPN solution terminates on a CISCO ASA head-end configured for client-based SSL VPN. AnyConnect Mobility Client is deployed to the endpoint mobile devices. Authentication is through RSA SecurID second factor authentication using software tokens. The RSA Authentication Manager 8.1 is configured in high availability mode (Active/Active) and runs within a virtual environment. The current client VPN and token software versions are listed below.

**Table N-4 Current Client VPN and Token Software versions**

	Software Versions VPN Client	Software Versions RSA Client
Windows	Anyconnect ver 4.10.00093	SID820 Software Tokens Ver 4.11
Mac	Cisco Secure Client (4.10.x)	N/A (App Store Version Used)
Apple IPAD	Cisco Secure Client (4.10x)	N/A (App Store Version Used)
Android	Cisco Secure Client (4.10.x)	N/A (Play Store Version Used)

SARS has a total of 11 500 RSA SecureID soft tokens of which 5 000 expire on 30 April 2024.

SARS may opt to augment or replace this service with a Zero Trust Network Access gateway, also known as a ZTNA controller or ZTNA broker, to provide secure remote access to applications and resources without exposing them to the public internet.

## 10.8 Firewall Support Services

SARS requires comprehensive support for firewalls and related security devices, ensuring availability, performance, and security. The Service Provider is required to take on and provide ongoing software and hardware maintenance of the implemented Cisco firewall technology within its data centres, and Internet perimeters and disaster recovery site. The support for the firewalls must be delivered according to the Device-based Service definitions, including the support and maintenance of the software and hardware comprising the firewall solution.

Firewall Analyser: SARS requires an analysis and compliance reporting solution with this service. The tool should be able to generate reports in several formats which include ISO/IEC 27001, Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), GDPR, Basel-II, etc.

Firewall management and orchestration: SARS may opt for a management tool, which gives a complete view of the network – on-premises, in the public, and private cloud. The tool should be capable of automating the management and configuration of multiple firewalls, security devices, and related network infrastructure components in a coordinated manner.

## 10.9 Security Assessments

The Service Provider is required to provide security assessments, penetration testing and vulnerability assessments on request by SARS. SARS currently performs these assessments annually to assist with improving the security posture of applications by way of application security assessments and subsequent post application assessment reviews following remediation. The focus of these assessments will be on all SARS internal-facing applications, although may have a wider scope.

Due to the highly specific and specialised nature of a security assessment, the Service Provider will be required to submit a proposal in response to a request from SARS, detailing the skills, knowledge and experience of the individuals proposed to conduct the assessment. The rates for personnel proposed by Service Provider must be in line with the personnel rates provided as part its response to the RFP. SARS, in its sole discretion, may accept or reject the proposal. The award of the RFP to the Service Provider is non-exclusive and SARS reserves its right to contract third parties to conduct security assessments.

SARS requires Digital Forensics and advanced Incident Response services in cases of a security breach or investigation. The service provider is required to provide this service on demand.

- **Incident Response:** Assist SARS to enhance and execute its incident response plan. This includes activities for identifying, containing, analysing, and eradicating the incident.
- **Digital Evidence Collection:** Collect and preserve digital evidence from the affected systems or devices. This involves the use of specialised tools and techniques to create a forensic image of the affected system or device to prevent data loss.
- **Digital Evidence Analysis:** Analyse digital evidence to determine the cause and extent of the security breach or incident. This involves examining system logs, network traffic, and other digital artifacts to identify any malicious activity.
- **Incident Mitigation:** Take immediate steps to contain the security breach or incident and prevent further damage. This may involve isolating affected systems, blocking network traffic, or disabling user accounts.
- **Remediation:** Develop a remediation plan to address any vulnerabilities or weaknesses that were exploited in the security breach or incident. This may involve patching software, updating security policies, or improving employee training.

- **Reporting and Documentation:** Document all aspects of the incident response process, including the incident itself, the steps taken to contain and remediate the incident, and any lessons learned. This documentation can be used to improve SARS's incident response plan and prevent future incidents.

#### 10.10 Network Admission Control

The Service Provider is required to take on and provide ongoing software maintenance and support of the Cisco Identity Services Engine (ISE), an identity-based network access control and policy enforcement system, previously known as the Network Admission Control solution. SARS also requires the Service Provider to provide additional licences as and when SARS so requires.

#### 10.11 Managed SOC Service

SARS requires a Managed SOC service to provide threat detection and response, security intelligence services, SIEM and SOAR capabilities and staff augmentation for an existing internal SOC.

**Threat Detection and Response:** The Managed SOC Service Provider must have a proven track record of providing comprehensive threat detection and response capabilities, including real-time monitoring of all security devices, continuous security log analysis, and proactive threat hunting to detect and respond to potential security incidents. A 24X7 CSIRT service is required with this service.

**Security intelligence:** The Managed SOC Service Provider must provide up-to-date threat intelligence and security analysis to keep SARS informed about the latest security threats, vulnerabilities, and attack trends. This includes regular security assessments and vulnerability scanning, as well as the ability to conduct deep-dive investigations into security incidents.

**Staff Augmentation:** The Managed SOC Service Provider must be able to provide experienced security professionals to work alongside the existing internal SOC team. This includes security analysts, incident response specialists, and other security experts with a proven track record of managing complex security environments.

**SOAR Capabilities:** The Managed SOC Service Provider must have Security Orchestration, Automation, and Response (SOAR) capabilities that can automate incident response processes, minimise response times, and reduce the risk of human error. The SOAR platform must be integrated with the SIEM and other security tools to enable automated threat detection and response.

**SLAs:** The Managed SOC Service Provider must provide clear and measurable SLAs for all services provided, including response times for security incidents and uptime guarantees for all security devices and systems. The SLAs must be based on industry best practices and regularly reviewed and updated to ensure they continue to meet SARS's needs.

**Compliance and Regulatory Requirements:** The Managed SOC Service Provider must have a thorough understanding of all relevant compliance and regulatory

requirements to ensure compliance with all requirements and must be able to provide regular reporting and auditing as required.

**Scalability and Flexibility:** The Managed SOC Service Provider must be able to scale their services up or down as required to meet the SARS's changing needs. They must be able to adapt their services to work with the existing security infrastructure and must be flexible in their approach to security management.

#### 10.12 **Micro-segmentation Platform**

SARS requires a comprehensive security and analytics platform designed to provide real-time insights into application behaviour and network traffic. The platform should be able to automatically discover and visualise all application components and their interdependencies across physical and virtual environments. Additionally, the platform should provide advanced security capabilities, including micro-segmentation, policy enforcement, and threat detection and response.

**Micro-segmentation:** The platform should enable administrators to create and enforce fine-grained policies that restrict communication between various parts of an application. This helps to prevent lateral movement of threats within the data centre and reduce the attack surface of the application.

**Application Dependency Mapping:** The platform should be able to provide a comprehensive application dependency mapping capability that can help administrators understand the behaviour of the application and its underlying infrastructure and make informed decisions about how to optimise performance and security.

**Policy Enforcement:** The platform should provide a centralised policy engine that allows administrators to define and enforce policies for application behaviour, network traffic, and user access. Policies should be able to be dynamically adjusted based on changing conditions.

**Threat Detection and Response:** The platform should use machine learning and behavioural analytics to detect and respond to threats in real time. It should continuously monitor application behaviour and network traffic, and automatically alert administrators to potential security incidents. It should also provide detailed forensics data that can be used to investigate and remediate incidents.

**Compliance and Governance:** The platform should provide a comprehensive compliance and governance framework that helps organisations meet regulatory requirements and industry standards. The platform should support auditing and reporting capabilities and be able to generate compliance reports for a variety of standards.

**Integration with Other Security Products:** The platform should integrate with other security products to provide a comprehensive security solution for the data centre and cloud. The solution must be able to integrate with other network and security solutions, such as routers and switches, firewalls, IDS/IPS, and SIEM solutions. It is important to note that the existing infrastructure is largely Cisco-based.

**Scalability and Multi-cloud Support:** The platform should support a variety of cloud environments, including public clouds like AWS and Azure, as well as private clouds

based on OpenStack and VMware. The platform should provide a consistent security policy across all environments, helping to simplify management and reduce risk. The solution must be scalable to accommodate growth in our network environment and be able to support our future business requirements.

**Analytics and Insights:** The platform should provide advanced analytics and insights into application behaviour and network traffic. It should be able to identify anomalous behaviour, diagnose performance issues, and optimise resource utilisation, helping to improve the overall efficiency and security of the data centre.

**Performance:** The solution must be able to provide high performance and low latency to ensure that there is no impact on our business operations.

**API Integration:** The platform should provide a comprehensive set of APIs that can be used to integrate the platform with other tools and systems, enabling organisations to automate security and operational processes.

**Deployment Architecture:** The solution must be able to support our existing network infrastructure. The solution should be deployed without any impact on our existing network environment

#### 10.13 Service Coverage Periods and Service Levels Applicable to Tower N

The specific Service Coverage Periods applicable to the Break-fix activities in Tower N are set out in Table N-5 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 the SARS 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.

**Table N-5: Service Coverage Periods applicable to Tower N**

Service Coverage Period	Period Covered
Basic	06:00 to 18:00 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 N are set out in Table N-6 below. Elapsed time to service restoration is only counted during the Service Coverage Period applicable to the device.

The detailed operation of Service Credits relating to Service Level failures is set out in Schedule C of the *Network, Server and End-user Device Support Services Agreement*.

**Table N-6: Service Levels applicable to Tower N**

**Break-fix Service Level Classes**

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

**Standard Chargeable Services: Service Levels**

Service	Time to Complete
Device IMACD	<p>(Two) 2 working days from works order approval (adding new/ non-service affecting)</p> <p>(One) 1 working day – Remote configuration (non-service affecting)</p> <p>Note: If client is requesting service to be rendered after hours (call to be placed in pending and then status to change once SP start with installation).</p> <p><b>Other:</b></p> <p>Wireless Surveys – 5 (five) working days from works order approval.</p> <p><b>No SLA (Change processes)</b></p> <p>Projects</p> <p>Service impacting</p> <p><b>Other (Not included in SLA)</b></p> <p>Specific items based on a requirement that can only be ordered once PO has been raised.</p>
Install network point (including cabling)	(Two) 2 working days for Metros and 4 (four) working days for other (from works order approval).



Service	Time to Complete
	<p>Client requesting service to be rendered after hours (call to be placed in pending and then status to change once SP start with installation).</p> <p><b>No SLA (Change processes)</b></p> <p>Cabling clean-ups.</p> <p>Cabling projects.</p> <p><b>Other (Not included in SLA)</b></p> <p>Specific items based on a requirement that can only be ordered once PO has been raised (example: specific power poles).</p>
Device Shipping	<p>(One) 1 working day (Metros) – Express/Overnight delivery.</p> <p>(One to two) 1-2 working days (Metros) – Expedited delivery.</p> <p>(Two to three) 2-3 working days (Border Posts/Towns) – Economic/Standard delivery.</p>

#### Other Services: Service Levels

Service	Time to Complete
Supply Quotes	<p><b>General</b></p> <p>(Two) 2 working days from receipt of request.</p> <p><b>Project</b></p> <p>(Five) 5 working days from receipt of request.</p>
OEM Contract Renewals	<p>(Five) 5 working days from works order approval (SP to provide notice of expiry of any OEM contract 90 (ninety) days before renewal is required).</p>

#### 10.14 Service Provider Technical Personnel

At Commencement Date and throughout the Term, the Service Provider's 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
Network General Equipment	CISCO certification (CCNP) and at least 3 (three) years of related and practical experience on general network equipment.

Device Category/Equipment Type	Service Provider Personnel Required certifications/experience
	CISCO Meraki certification (ECMS1 and 2) and at least 3 (three) years of related and practical experience on Meraki equipment.
Network Specialised Equipment	CISCO certification (CCIE) and at least 5 (five) years of related and practical experience on specialised network equipment (e.g., CISCO ACI, CISCO Datacentre Switches).
F5 Load Balancers	F5 certification (301 A+B) and at least 5 (five) years of related and practical experience on Big IP LTM.
Voice General Equipment, including Software	<p>CISCO certification (CCNP) and at least 3 (three) years of related and practical experience on voice equipment.</p> <p>Yealink certification (CIPPE Senior) and at least 1 (one) year of related and practical experience on Yealink equipment.</p> <p>Poly certification towards integration with MS Teams and Zoom) and at least 1 years related and practical experience on Poly equipment.</p> <p>MS Teams certification (Microsoft 365 Certified: Teams Administrator Associate).</p> <p>Zoom (As specified by OEM).</p> <p>Webex and Jabber (CISCO certification (CCNP)).</p>
Network General Equipment	<p>CISCO certification (CCNP) and at least 3 (three) years of related and practical experience on general network equipment.</p> <p>CISCO Meraki certification (ECMS1 and 2) and at least 3 (three) years of related and practical experience on Meraki equipment.</p>
Project Management Services	Project Management Certification and at least 5 (five) years of related and practical experience.
Network Security VPN (RAS)	CISCO Certification CCIE with at least 5 (five) years of related and practical experience on the RSA appliances. (for second –level support).
Network Security Services (CISCO ASA firewall, ACS appliances/ISE software)	CISCO certification (CCIE) with at least 5 (five) years of practical and related security experience on firewalls.
Fraud and Phishing Detection and Security Assessment Services	Technical Account Manager with at least 5 (five) years of related and practical experience in managing technical service providers (e.g., Anti-phishing and security assessment services).
Network Admission Control	CISCO certification (CCIE) with at least 5 (five) years of practical and related security experience on NAC.
PADS4	PADS4 certification with at least 3 (three) years of practical and related PADS4 infrastructure experience
SOC	Certified level 3 SOC analysts with at least 5 (five) years of practical experience in a fully managed SOC.

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

In addition to the Seats that will be made available for Key Service Provider Personnel as described in paragraph 6.15 and Service Management personnel described in paragraph 9.15, SARS will make additional Seats available as set out in Table N-7 to the Service Provider for Tower N services.

**Table N-7. Number of Seats provided by SARS for use by Service Provider**

Function	Site	Number
Administrator (Billing / Stores / Cmdb)	Lehae La SARS	2
Network Engineer	Alberton	1
Network Engineer	Doringkloof	1
Network Engineer	Lehae La SARS	5
Project Manager	Lehae La SARS	0
Security Engineer	Lehae La SARS	2
AV Engineer	Lehae La SARS	2
PADS4 Engineer	Lehae La SARS	1

The Service Provider must ensure that sufficient personnel is 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.

#### 10.15 Professional Services

From time to time during the Term, SARS may require professional services from the Service Provider which must be provided on request in line with the personnel rates provided as part its response to the RFP. Professional services may be required from the Service Provider, encompassing any field relating to the scope of Network Support Services including IT Security Support Services.

The following Professional Services (Full Time Engineers/Resources services [FTE's]) are required at Commencement Date and must form part of the Transition of services to the new Service Provider. The Bidder is encouraged to transfer the below critical staff from the current Service Provider to minimise operational risk:

- CISCO Senior ACI Engineer;
- CISCO Senior LAN Engineer (including Cisco Meraki);
- CISCO Senior Wireless Engineer;
- CISCO Security Engineer (Firewall, ISE);
- F5 Senior Engineer;
- Application Performance Management Engineer; and
- SOC analysts (x2).

The non-critical resources listed below are also required from Commencement Date:

- F5 Engineer;
- PADS4 Engineer;
- Store Administrator;
- Network Management Engineer (Tools);
- CISCO Senior Voice Engineer;
- CISCO Junior Wireless Engineer; and
- Network and Application Monitoring and Performance Engineer.

Network support on Microsoft Teams and Zoom and support and services from Cisco Meraki Eco Partners will be required during the contract term as/when requested.

## 11 TOWER S: SERVER SUPPORT SERVICES

### 11.1 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, IBM intel-based servers, including hardware support.
- Procurement and other services
  - Non-exclusive procurement of Server consumables not limited 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, maintenance services;
  - c. Supply of server consumables;
  - d. Professional services;
  - e. The provision of Standard Chargeable Services such as install, move, add, change and decommissioning services; and
  - f. 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.

SARS may require the Service Provider to perform inventory checks.

SARS may require the Service Provider to provide courier services.

SARS may request for 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 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.

## 11.2 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 now include additional services such as the inclusion of support for additional device types.

## 11.3 Transition

The Service Provider appointed in Tower S is required to complete the Transition Services within 3 (three) months from the Effective Date. By the end of the 3 (three) months, 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 Support Services Agreement, the Service Provider must have:

- Fully designed, developed, implemented the signed-off processes, procedures, schedules and work practices detailed in the Network, Server and End-user 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 Network, Server and End-user 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 Network, Server and End-user 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 Network, Server and End-user Device support services 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. If 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.

#### 11.4 **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, makes 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. With 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 Server and Server Equipment**

Category	Description / notes
<b>Server Computing Devices</b>	
Server (Intel) Dell PowerEdge R710 Dell PowerEdge R720 Dell PowerEdge R730 Dell PowerEdge R740XD Dell PowerEdge R740 Dell PowerEdge R750 Dell PowerEdge R920 Dell PowerEdge R930 Dell PowerEdge R940 Dell PowerEdge R240 IBM X-Series 3650 M4 IBM X-Series 3850 M5	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	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,
<b>Server Peripherals/Miscellaneous</b>	
KVM Console	KVM console and keyboard for server rack configuration.
KVM Switch	KVM switch for multiple server management.
Server rack	Server rack including power supply.

**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					
<ul style="list-style-type: none"><li>• Server (Intel)</li><li>• Server Blade</li><li>• Blade Chassis (Intel), including on board switches</li><li>• Server (shared infrastructure platform)</li></ul>	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.
Server rack	n/a	n/a	SARS-provided Swap-out device	n/a	The Swap-out service includes the Swap-out of PDUs within the server rack and cabinet relocation.

### 11.5 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 Network, Server and End-user 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.

#### 11.6 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 more than 2 (two) years of experience CompTIA A+, N+, Server+ certifications; MCP (Microsoft Certified Product – Server) qualification and OEM certification on servers, blades, and at least 2 (two) years of experience. Cloud certification.
General Computer Device Engineer	OEM certification with more than 2 (two) years of experience).
Project Management Services	Project Management Certification and at least 5 (five) 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.

In addition to the Seats that will be made available for Key Service Provider Personnel as described in paragraph 6.15 and Service Management personnel described in paragraph 0, SARS will make the following Seats available to the Service Provider for Tower S services:

**Table S-5 Number of Seats provided by SARS for use by Service Provider**

Function	Site	Number
Server Engineer	Lehae La SARS	2
Server Engineer	Revenue - Alberton Campus	00
Server Engineer	Revenue - Bellville	00
Server Engineer	Revenue - Doornkloof Contact Centre	00
Server Engineer	Revenue - Trescon House	00
Operations Manager	Lehae La SARS	1

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.

#### 11.7 Professional Services

From time to time during the Term, SARS may require professional services from the Service Provider which must be provided on request in line with the personnel rates provided as part its response to the RFP. Professional services may be required from the Service Provider encompassing any field relating to the scope of Server Support Services.

## 12 TOWER E: END-USER DEVICE SUPPORT SERVICES

### 12.1 Scope

The scope of SARS requirement for Tower E: End-user Device Support Services comprises nationwide provision of the following:

- End-user device support services (Device-based Services, Standard Chargeable Services, project, consulting and training) for SARS-owned and SARS-managed End-user Devices, including hardware support.
- Multifunction Printer support services (Device-based Services, Standard Chargeable Services, project, consulting and training) for SARS-owned and SARS-managed Multifunction Printer, including hardware support.)
- Supply of consumables for applicable devices.
- Management of OEM and Third-Party Supplier support contracts.
- The common services set out in paragraph 6, including service management, service provider management personnel, administration, research and development, consulting, project management and support.

The services, at a high level, comprise the management of incidents, the provision of defined services relating to the supported equipment, maintenance services; supply of consumables; professional services; the provision of Standard Chargeable Services such as install, move, add, change and decommissioning services; and compliance with required service management procedures.

### 12.2 Delivery Model

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

### 12.3 Transition

The Service Provider appointed in Tower E is required to complete the Transition Services within 3 (three) months from the Effective Date. By the end of the 3 (three) months, the Service Provider must have assumed full management responsibility for the full scope of End-user Device Support Services. In addition to any other commitment required in the Network, Server and End-user Device Support Services Agreement, the Service Provider must have:

- Verified the warranty status of all End-user Devices;

- Fully designed, developed, implemented the signed-off processes, procedures, schedules and work practices detailed in the Network, Server and End-user Device Support Services Agreement, especially those detailed in Schedule B-E and its attachments;
- Committed to reporting and meeting Service Levels as set out in Schedule C and Appendices C-E-1 and C-E-2 of the Network, Server and End-user 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 Network, Server and End-user Device Support Services Agreement;
- Developed and established the necessary interfaces with other SARS service providers required for the delivery of End-user Device Support Services;
- Taken over the management of end-user device 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 End-user 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.

## 12.4 Device-based Services applicable to Tower E

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

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

- Tower E Site Classifications;
- Tower E End-user Device Categories and Quantities; and
- Tower E End-user Device per SARS Site.

One of the objectives of this RFP is to achieve flexibility in the procurement of services. In this regard, Table E-2 sets out the Break-fix services SARS may require during the Term. The Bidder is required to provide rates for all required services for each End-user device category as 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 E Pricing Response Template for the details of rates that must be supplied by the Bidder.

During contract finalisation, SARS will make an election for 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 Passport Scanners. SARS may, during contract finalisation, elect to contract for Break-fix services (In-warranty) and Break-fix services (Out-of-warranty) for this type of device. With 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 E-1: Categories and types of End-user Devices**

Category/type	Description/notes
<b>End-user Computing devices</b>	
Desktop (Wintel)	Includes the desktop computer, motherboard, casing, power supply, memory, data storage device, display adaptor(s), keyboard and mouse. This category excludes all Apple desktop devices. Note that this excludes the display/screen.
Desktop (Apple)	Includes the desktop computer/display, motherboard, casing, power supply, memory, data storage device, display adaptor(s), keyboard and mouse. This category only includes Apple desktop devices. Note that this excludes the display/screen unless it is an integrated unit.
Laptop (Wintel)	Includes the laptop computer/display, motherboard, casing, power supply, memory, data storage device, display adaptor(s), keyboard and mouse. This category excludes all Apple laptop devices. Note that this excludes docking stations associated with laptops.
Laptop (Apple)	Includes the laptop computer/display, motherboard, casing, power supply, memory, data storage device, display adaptor(s), keyboard and mouse. This category only includes Apple laptop devices.
Tablet (Wintel)	Includes the tablet computer/display, motherboard, casing, power supply, memory, data storage. This category includes all Wintel tablet devices.
Tablet (Apple)	Includes the tablet computer/display, motherboard, casing, power supply, memory, data storage. This category includes all Apple tablet devices, e.g., iPad, devices.
Tablet (Android)	Includes the tablet computer/display, motherboard, casing, power supply, memory, data storage. This category includes all tablets other than Wintel and Apple devices.



Display Devices	
Computer Monitors	The support for computer monitors (e.g., LED/LCD monitors) is separately charged from the computer device. The support for these devices includes the display cabling.
Wall-mounted Monitors	Wall mounted monitors/televisions (large format). The support for wall mounted monitors (e.g., plasma, LED, LCD or later technologies) includes the cabling and associated devices such as splitter boxes.
Data Projectors	Includes the projector cabling and any other projecting systems.
Interactive White Boards	Includes the cabling, built-in printer mechanisms, screen rollers, etc.
All-In-Ones (AIO)	Display units that integrate all computer processing components into a single unit chassis. This design eliminates the need for a separate computer tower.
Wearable (VR and AR)	Any device that overlays digital information onto user's physical environment. Virtual Reality and Augmented Reality.
Digital Signage Equipment	Display systems for creating and managing dynamic content on digital screens, such as advertising, wayfinding, or informational displays.
VGA Splitter Box	Output signal splitting devices.
Input Devices	
Biometric Fingerprint Scanners	Biometric fingerprint scanner for the purpose of personal identification.
Handheld Barcode Scanner	Devices used for reading of asset and document barcodes.
Signature Pads	Purpose built devices used for the capturing of signatures.
Camera	Hand-held or mounted cameras for the capture of still sequences or motion video and facial recognition (this excludes security surveillance [CCTV] cameras)
Personal Document Scanners	Standalone document scanners are low volume document scanners directly attached (USB or other direct cable attachment) to a computing device. These are generally for the use by a single workstation.
Biometric capable Mice	Mouse that can do fingerprint reading for biometric authentication on Endpoints.
Gesture Controllers	Devices that capture user movements and gestures to interact with computer systems such motion controllers and depth sensing cameras.
Bulk Document Scanner	High-speed scanning devices designed for digitising large volumes of paper documents.
Passport Scanner	Purpose built devices used for the scanning of machine-readable passports.
Printing Devices	
Barcode Printer	Locally attached (USB) printer devices used specifically for the purpose of printing barcodes.

Printing Devices	
Braille Printer	Locally attached (USB) printer devices used specifically for the purpose of printing Braille documents.
Label Printer	Locally attached (USB) printer devices used specifically for the purpose of printing labels.
Thermal Receipt	Locally attached (USB or other cable attachment) printer device using thermal printing technology for the printing of receipts.
Document Printer	Locally attached (USB or other cable attachment) printer devices using laser, dot matrix or inkjet technology (includes mobile printers).
Personal MFD	Locally attached (USB or other cable attachment) multifunction device primarily for printing, faxing and scanning.
Multi-Functional Printers (MFPs)	Network attached multi-function Printer primarily used for bulk printing, scanning and copying.
3D Printer	Locally attached (USB or other cable attachment) or networked printer devices used for additive manufacturing, creating three-dimensional objects.
Plotter	Locally attached (USB or other cable attachment) plotting device.
Miscellaneous Computing Devices	
Mi-Fi (Mobile Wi-Fi) devices	Battery-powered mobile hotspots that create a localised Wi-Fi network by connecting to cellular data networks (e.g., 4G or 5G).
Wi-Fi Dongles	Also known as Wi-Fi adapters or USB Wi-Fi adapters, are small devices that plug into a computer's USB port to provide Wi-Fi connectivity. They are typically used to enable Wi-Fi capabilities on devices that do not have built-in Wi-Fi, such as desktop computers or older laptops.
Consumables	
Keyboard (including wireless)	USB attached keyboard. Note that keyboards that are replaced as part of a Break-fix process are not to be charged as consumables and must be included in the In- or Out-of-warranty monthly rates and standard chargeable support costs
Biometric Mouse (including wireless)	Optical USB attached mouse. Note that mice that are replaced as part of a Break-fix process are not to be charged as consumables and must be included in the In- or Out-of-warranty monthly rates and standard chargeable support costs.
Digital pens and styluses	Devices used for drawing, writing, and navigating on touch-enabled devices, such as tablets, touchscreens, and digital drawing pads. Note that Pens and Styluses that are replaced as part of a Break-fix process are not to be charged as consumables and must be included in the In- or Out-of-warranty monthly rates and standard chargeable repair costs.

Consumables	
Memory Stick and Micro SD Card	8/16/32/64/128/256 GB. These must be supplied on request on a Time and Materials basis.
Fly leads	2m/5m network fly leads. These must be supplied on request on a Time and Materials basis.
Solid State Drive	512GB and 1TB High performance storage device for laptops and desktops. (Internal and External Drives). These must be supplied on request on a Time and Materials basis.
Memory Module	8GB/16GB RAM modules. These must be supplied on request on a Time and Materials basis.
Printer Toner	Black and Colour Toners. These must be supplied on request on a Time and Materials basis.
Printer Staples	Stapler cartridges. These must be supplied on request on a Time and Materials basis.

**Table E-2: Detailed Description of Required Break-fix Services Applicable to Device Categories**

Category	Break-fix Services				Notes
	In-warranty	Out-of-warranty	Swap-out	Service-only	
End-user Computing devices					
Desktop (Wintel) Desktop (Apple) Laptop (Wintel) Laptop (Apple)	SP-provide d WUS	SP-provided WUS	SARS provided Swap-out unit	n/a	<p>All devices must be repaired on or offsite. The Service Provider may take devices offsite provided that all data backups and sanitisations are completed.</p> <p>The Service Provider must provide a WUS to meet the Service Levels.</p> <p>Service and the rates must include the Swap-out of faulty mouse and keyboard.</p>
Tablet (Wintel) Tablet (Apple) Tablet (Android)	SP-provide d WUS	SP-provided WUS	SARS-provided Swap-out unit	n/a	<p>All devices may be repaired on or offsite. The Service Provider must provide a Whole Unit Spare to meet the Service Level.</p> <p>Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.</p>

Category	Break-fix Services				Notes
	In-warranty	Out-of-warranty	Swap-out	Service-only	
Display Devices					
Computer Monitors	SP-provided WUS	SP-provided WUS	n/a	n/a	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level.
Wall mounted Monitors	SP-provided WUS	SP-provided WUS	n/a	No WUS applicable	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level where indicated.
Data Projectors	SP-provided WUS	SP-provided WUS	n/a	No WUS applicable	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level where indicated.
Interactive White Boards	No WUS	n/a	n/a	No WUS applicable	All devices may be repaired on or offsite. No WUS services are required.
All-In-One (AIO)	SP-provided WUS	SP-provided WUS	n/a	n/a	All devices may be repaired on or offsite.
Wearable (VR and AR)	No WUS	No WUS	SARS-provided Swap-out Unit	n/a	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level. Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.
Digital Signage Equipment	No WUS	No WUS	n/a	No WUS applicable	All devices may be repaired on or offsite.
VGA Splitter Box	SP-provided WUS	n/a	n/a	No WUS applicable	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level where indicated.

Input Devices					
Biometric Fingerprint Scanners/Handheld Barcode Scanner/Signature Pads/Cameras	SP-provided WUS	SP-provided WUS	SARS-provided Swap-out unit	n/a	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level. Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.
Personal Document Scanners	No WUS	No WUS	n/a	No WUS applicable	All devices may be repaired on or offsite.
Passport Scanner	SP-provided WUS	SP-provided WUS	SARS-provided Swap-out unit	No WUS applicable	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level. Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.
Biometric capable Mice	SP-provided WUS	SP-provided WUS	SARS-provided Swap-out unit	No WUS applicable	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level. Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.
Gesture Controllers	No WUS	No Wus	n/a	No WUS Applicable	All devices may be repaired on or offsite.
Bulk Document Scanner	No WUS	No Wus	n/a	No WUS Applicable	All devices may be repaired on or offsite.
Printing Devices					
Barcode Printer Braille Printer Label Printer Thermal Receipt	SP-provided WUS	SP-provided WUS	SARS-provided Swap-out unit	No WUS applicable	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level. Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.
Document Printer	SP-provided WUS	SP-provided WUS	n/a	No WUS applicable	All devices may be repaired on or offsite. The Service Provider must provide a WUS to meet the Service Level where indicated.
Personal MFD	n/a	n/a	n/a	No WUS applicable	All devices may be repaired on or offsite. No WUS services are required.
Multi-Functional Printers (MFPs)	SP-provided Loan Unit	SP-provided Loan Unit	n/a	n/a	All devices may be repaired on or offsite. The Service Provider must provide a Loan Unit device to meet the Service Levels were indicated.
Plotter	n/a	n/a	n/a	No WUS applicable	All devices may be repaired on or offsite.
3D Printer	n/a	n/a	n/a	No WUS applicable	All devices may be repaired on or offsite.

Miscellaneous Computing Devices					
Mi-Fi (Mobile Wi-Fi) devices	n/a	n/a	SARS-provided Swap-out unit	No WUS applicable	Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.
Wi-Fi Dongles	n/a	n/a	SARS-provided Swap-out unit	No WUS applicable	Where SARS has elected for the Service Provider to provide a Swap-out service, SARS will provide the Swap-out unit.
Consumables					
Keyboard	n/a	n/a	SP-provided Swap-out unit	n/a	SP to carry Swap-out units.
Wireless Mouse	n/a	n/a	SP-provided Swap-out unit	n/a	SP to carry Swap-out units.
Biometric capable Mouse	n/a	n/a	SP-Provided Swap-out unit	n/a	SP to carry Swap-Out units.
Digital pens and styluses	n/a	n/a	SP-Provided Swap-out unit	n/a	SP to carry Swap-Out units.
Memory Stick and Micro SD Card	n/a	n/a	SP-Provided Swap-out unit	n/a	SP to carry Swap-Out units.
Fly leads	n/a	n/a	SP-Provided Swap-out unit	n/a	SP to carry Swap-Out units.
Laptop Battery	n/a	n/a	SP-Provided Swap-out unit	n/a	SP to carry Swap-Out units.
Solid State Drive	n/a	n/a	SP-Provided Swap-out unit	n/a	SP to carry Swap-Out units.
Memory Module	n/a	n/a	SP-Provided Swap-out unit	n/a	SP to carry Swap-Out units.

Printer Toner	n/a	n/a	SP- Provided Swap-out unit	n/a	SP to carry Swap-Out units.
Printer Staples	n/a	n/a	SP- Provided Swap-out unit	n/a	SP to carry Swap-Out units.

## 12.5 Service Coverage Periods and Service Levels applicable in Tower E

The specific Service Coverage Periods applicable to the Break-fix activities in Tower E are set out in Table E-3 below:

**Table E-3: Service Coverage Periods Applicable to Tower E**

Service Coverage Period	Period Covered
WFH	07:00 to 17:00 on weekdays only, public holidays are excluded.
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 E are set out in the Table E-4 below. Elapsed time to service restoration is only counted during the Service Coverage Period applicable to the device.

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.

The detailed operation of Service Credits relating to Service Level failures is set out in Schedule C of the Network, Server and End-user Device Support Services Agreement.

**Table E-4: Service Levels Applicable to Tower E****Break-fix Service Level Classes**

Service Level Class	Time to Repair
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.
Platinum	Service restoration within 2 (two) hours of the ticket being assigned to Service Provider.

**Standard Chargeable Services Levels**

Service	Time to Complete
Single Device IMACD	(One) 1 business day (completed on or before the same time of day as the request was made to the Service Provider on the next business day). If the request was made on a non-business day, the request will be regarded as having been logged at the start of the next business day.
2-10 Devices IMACD (Low Volume)	(Three) 3 business days.
11-50 Devices IMACD (Medium Volume)	(Five) 5 business days.
51-100 Devices IMACD (High Volume)	(Ten) 10 business days.
100+ Devices IMACD (Very High Volume)	To be negotiated based on the complexity and specific needs.

**12.6 Volume Based IMACD**

To ensure cost-effective delivery of volume-based requests versus single IMACD requests, the Service Provider must adhere to the following requirements:

**Volume Metrics:** The Service Provider must establish and implement volume metrics to accurately measure and track the quantity of IMACD requests processed. These metrics should allow SARS to monitor the efficiency and cost-effectiveness of the IMACD services provided.

**Tiered Pricing:** The Service Provider must offer tiered pricing structures for IMACD services, providing discounts for bulk requests to incentivize cost-effective and efficient management of volume-based IMACD tasks. The pricing structure should



be clearly defined and transparent, enabling SARS to easily understand and compare costs between single and volume-based requests.

**Process Optimisation:** The Service Provider must continuously review and optimise the IMACD processes, leveraging best practices from the ITIL framework to streamline operations and improve cost efficiency. This may include identifying opportunities for automation, implementing standardised procedures, and refining workflows to reduce redundancies and enhance overall productivity.

**Reporting and Analytics:** The Service Provider must provide regular reporting and analytics on the performance of IMACD services, including data on volume-based requests, cost savings achieved through discounts, and other relevant performance indicators. This information will enable SARS to assess the effectiveness of the volume-based IMACD rates and identify areas for improvement.

## 12.7 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
End-user Computing Devices	A+ and OEM certification and at least 2 (two) years of experience.
Multifunction Printing Devices	A+ and OEM certification and at least 2 (two) years of experience.
Project Management Services	Project Management Certification and at least 5 (five) years of experience.

Generally, all technical personnel must be familiar with basic service management processes, preferably a foundational level qualification and must possess the basic skills described in Table E-6. The Service Provider must ensure that for each SARS site, a qualified End-user Device support technician is able to provide services for the equipment located at that SARS site within the specified Service Levels.

The technical personnel should have expertise in network infrastructure and security, data backup and recovery procedures, and the latest trends and developments in end-user device technology. Technical personnel should also stay up to date with the latest training and education to ensure they can provide the best possible support to SARS end-users, while also adhering to organisational processes, policies and guidelines.

**Table E-6 Service Provider Personnel Foundational Skills and Knowledge**

Support Personnel Skills	Description
Technical Skills	Ability to diagnose and troubleshoot hardware issues, perform upgrades and repairs, configure and install software, and maintain inventory of devices. Familiarity with relevant tools, technologies, and software such as Active Directory, SCCM, Intune and Remote Desktop Services.
Communication Skills	Excellent communication skills, both written and verbal, with the ability to explain technical issues to non-technical users.
Teamwork	Ability to work effectively in a team environment, collaborating with other support personnel and SARS IT staff to resolve issues and complete projects.
Customer Service	Strong customer service orientation, with a focus on providing a positive end-user experience.
Attention to Detail	Strong attention to detail, with the ability to document procedures and maintain accurate inventory records.
Physical Requirements	Ability to lift and move equipment weighing up between 20 and –30 kg, and the ability to work in cramped or awkward spaces.

The Service Provider must ensure sufficient personnel are provided to meet the contractual performance standards, including the Service Levels, with a minimum dependency of seats provided by SARS. Consideration will be given to seating requests (To a maximum of two seats) at Platinum sites only. The Service Provider must monitor the utilisation of the allocated 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.

## 12.8 Professional Services

### Scope of Services

The Service Provider agrees to provide professional services to SARS on request, in accordance with the personnel rates specified in its response to the RFP. The professional services may cover any area related to the End-user Support Services, as defined in the RFP.

**Transition of Services**

As part of the transition of services to the new Service Provider, the following critical resources (Full Time Engineers/Resources) are required at the Commencement Date:

- **End-user Support Service desk engineers;**
- **Problem Management coordinators; and**
- **Technical Logistics Co-ordinator.**

The Service Provider is encouraged to transfer the critical resources from the current Service Provider to minimise operational risk.

**13 AWARD OF MORE THAN ONE TOWER TO A SERVICE PROVIDER**

The Proposals for Tower N, Tower S and Tower E will be evaluated and awarded separately. If more than one (1) Tower is awarded to a single Service Provider, SARS and such Service Provider will be able to benefit from efficiencies by eliminating functions that may be duplicated across the Towers so awarded.

It is expected that such operational efficiencies would be gained by eliminating duplications of scope. Examples where scope may be reduced are listed below:

- Only one Account Executive and one Service Delivery Manager need be provided to cover the scope of more than one Tower.
- A single Transition project management structure to cover the scope of more than one Tower.
- Resourcing efficiencies to fulfil service management obligations.
- Warehousing facilities may be shared across more than 1 (one) Tower.

In the event of an award of more than 1 (one) Tower being made to a Service Provider, SARS reserves the right to reduce the duplicated elements of scope through negotiations for commensurate reductions in the price quoted for such duplicated items of scope. The Service Provider will be required to negotiate in good faith and is required to disclose the cost drivers and cost make-up of the duplicated functions to achieve the most cost-effective solution for SARS.

## 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.

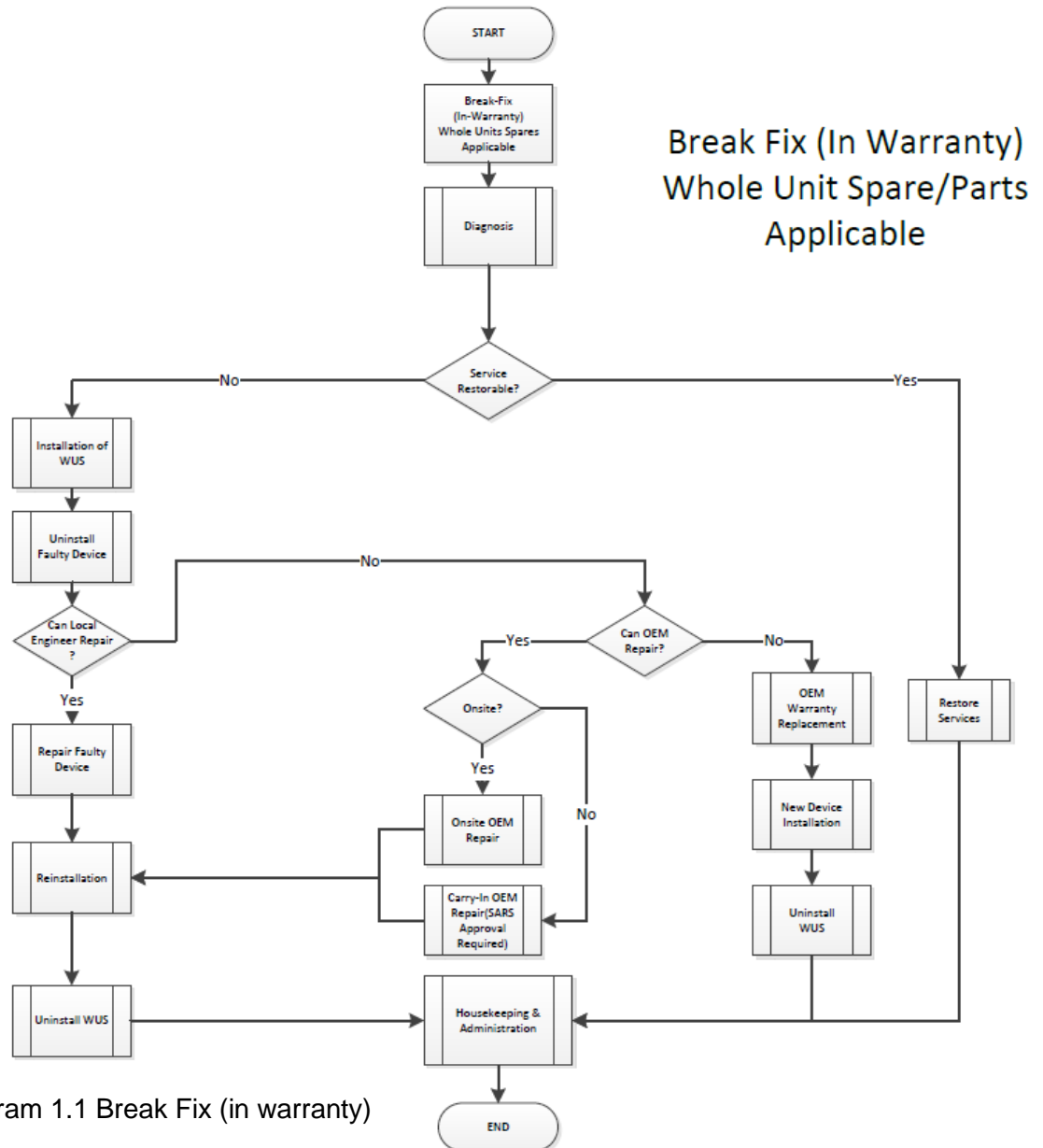
The Bidder must read these process flow diagrams in conjunction with provisions set out in *Schedule B of the Network, Server and End-user Device Support Services Agreement* and this Business Requirements Specification and supplement them with any activities that are regarded as necessary in terms of 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 a specific Tower the process flow will be reviewed and finalised during the Transition.

.

## 1 IN-WARRANTY BREAK-FIX PROCESS (WUS APPLICABLE)

The flowchart set out immediately below describes the process to be followed for the repair of In-warranty device service for devices that are required to be repaired onsite (Carry-in to OEM Repair only on SARS approval) and, if required to meet the Service Levels, the provision of a WUS. The Bidder must supply a monthly rate to facilitate co-ordination of warranty repair. No additional charges would be payable by SARS to effect the repair other than the monthly rate.



## 2 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 repair other than the monthly rate.

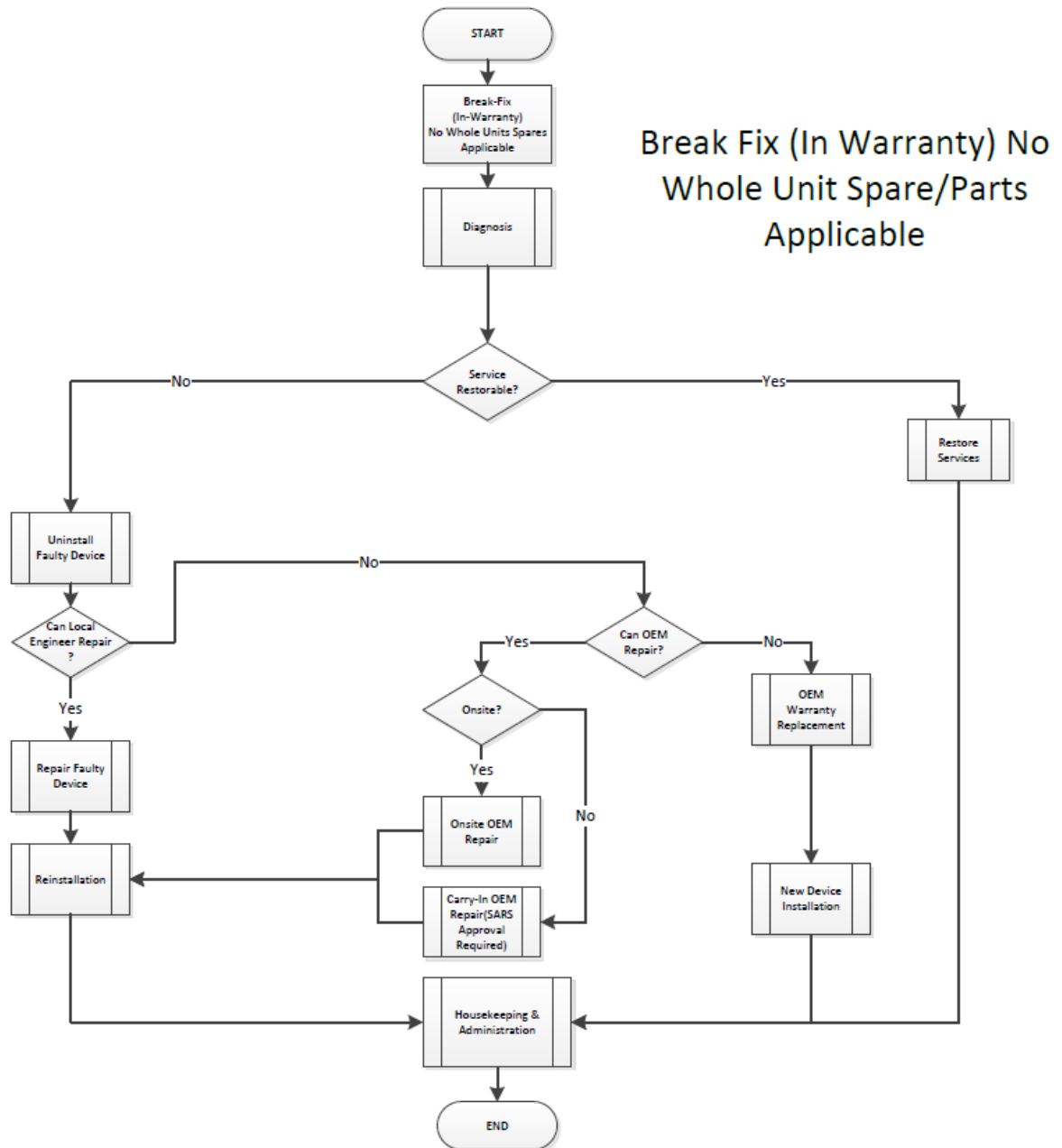


Diagram 2.1 Break Fix (in-warranty)

### 3 OUT-OF-WARRANTY BREAK-FIX PROCESS (WUS APPLICABLE)

The flowchart set out immediately below describes the process to be followed for the repair of Out-of-warranty devices that are required to be repaired onsite and, if required to meet the Service Levels, the provision of a WUS. The Bidder must provide a monthly rate. No additional charges are payable by SARS other than the monthly charge.

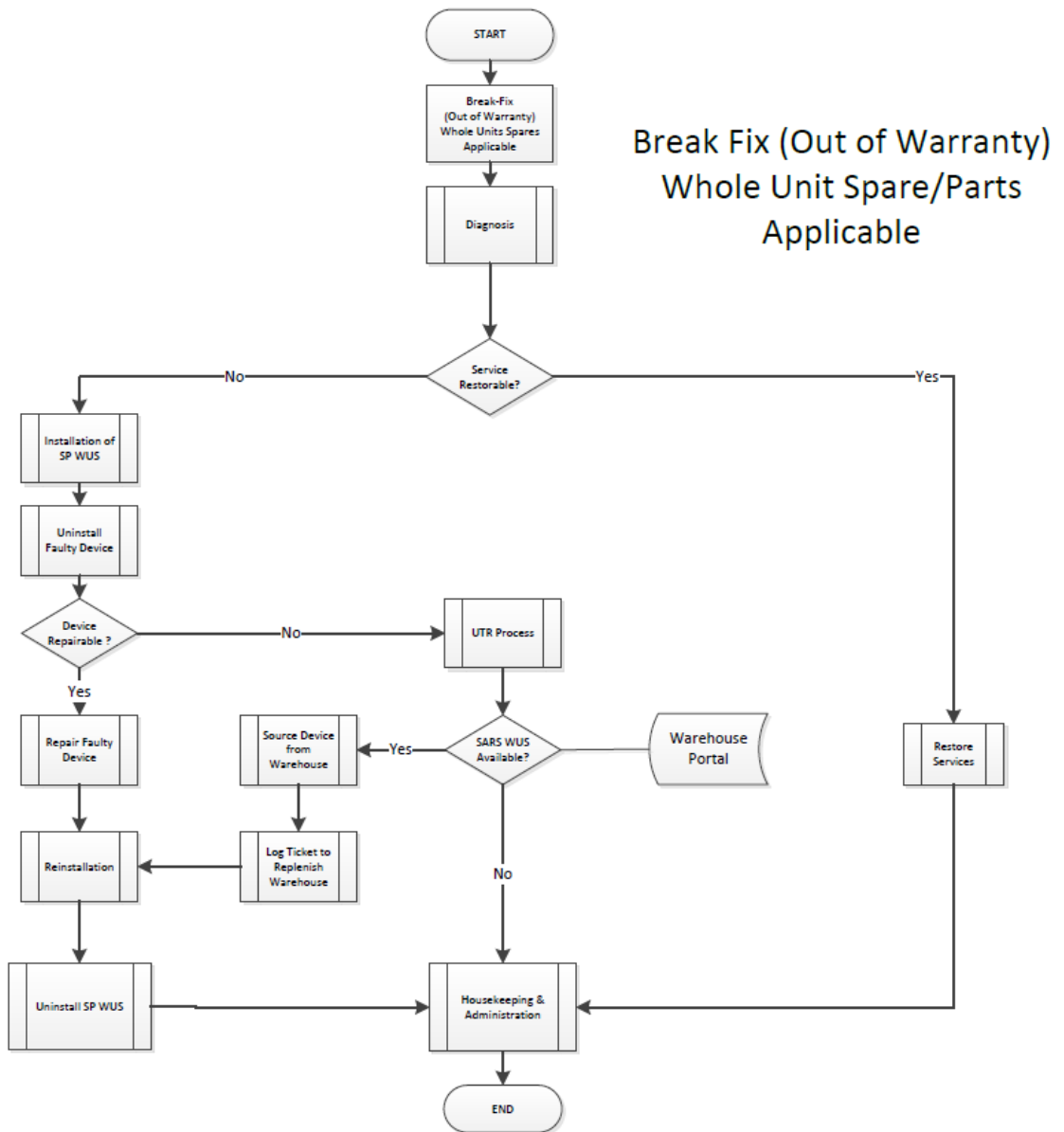


Diagram 3.1 Break Fix (out of warranty)

#### 4 SWAP-OUT REPAIR PROCESS

The flowchart set out immediately below describes the process to be followed for the Swap-out of non-functioning devices with a WUS. The Bidder must supply a monthly price to effect the repair. No additional charges are payable by SARS to effect the Swap-out other than the monthly rate.

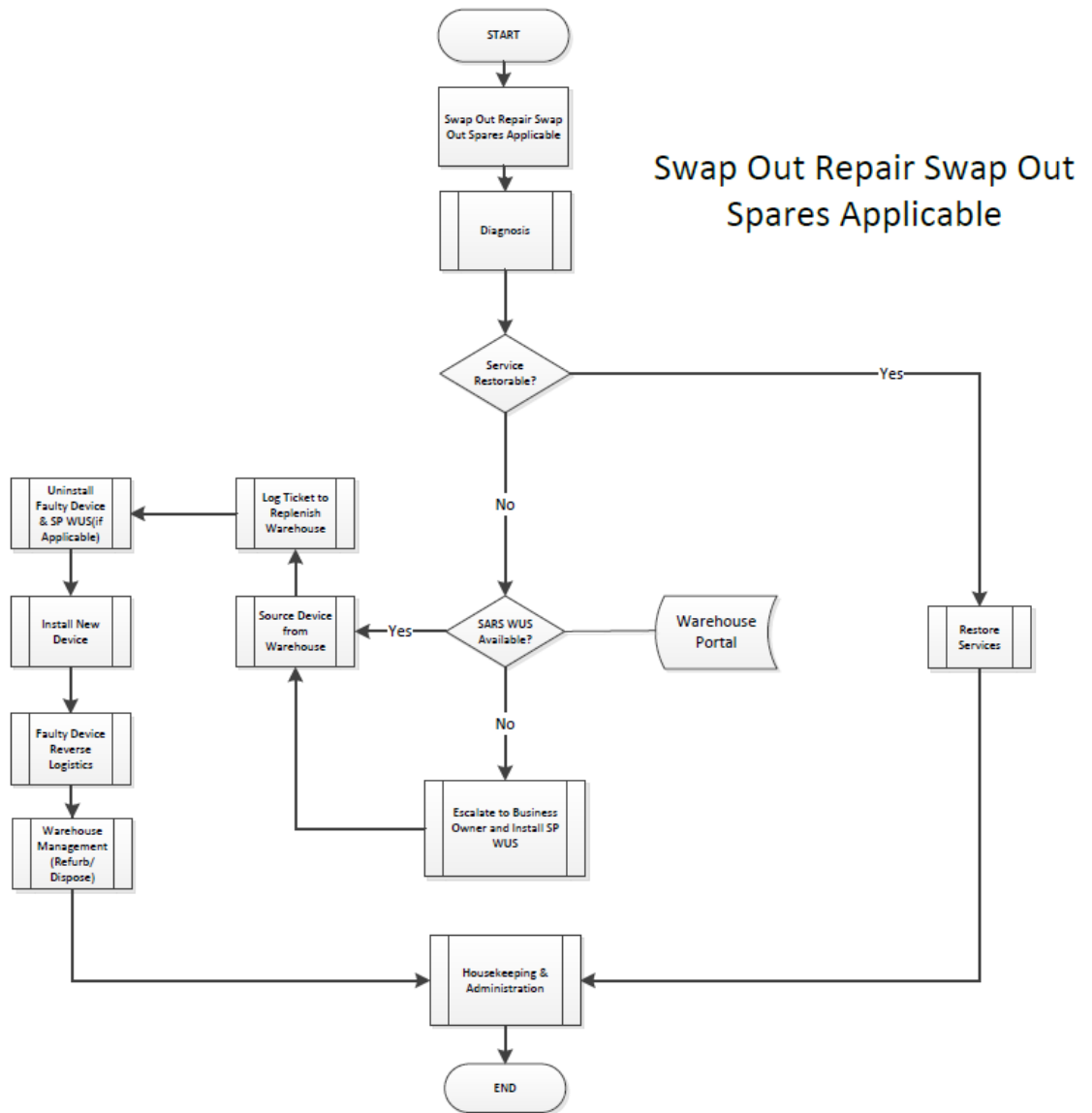
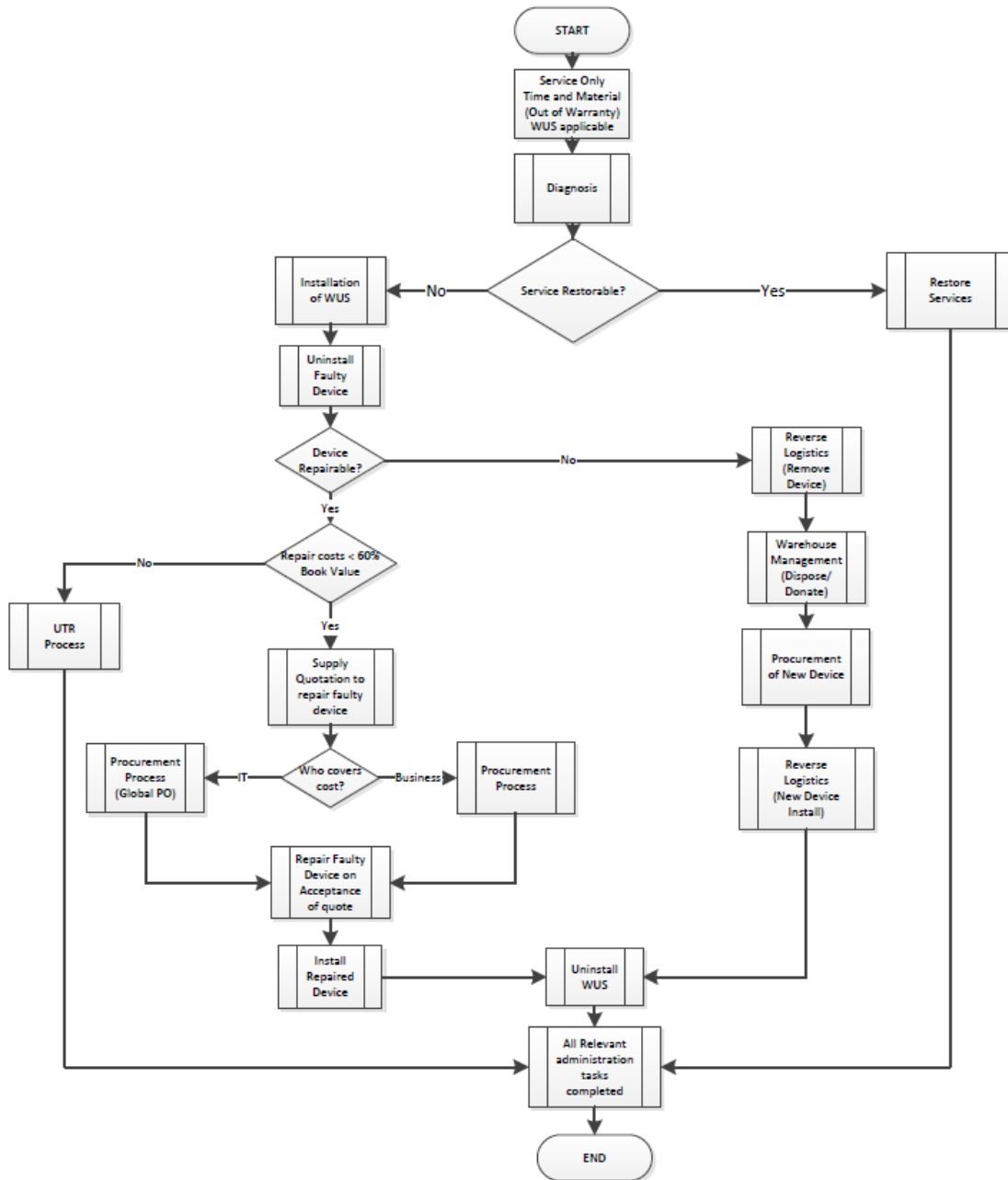


Diagram 4.1 Swop-Out Repair Process



## 5 SERVICE-ONLY – TIME AND MATERIAL PROCESS (WUS APPLICABLE)

The flowchart set out immediately below describes the process to be followed for the repair of Out-of-warranty devices that are fully covered by the monthly rate and, if required to meet the Service Levels, the provision of a WUS. 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

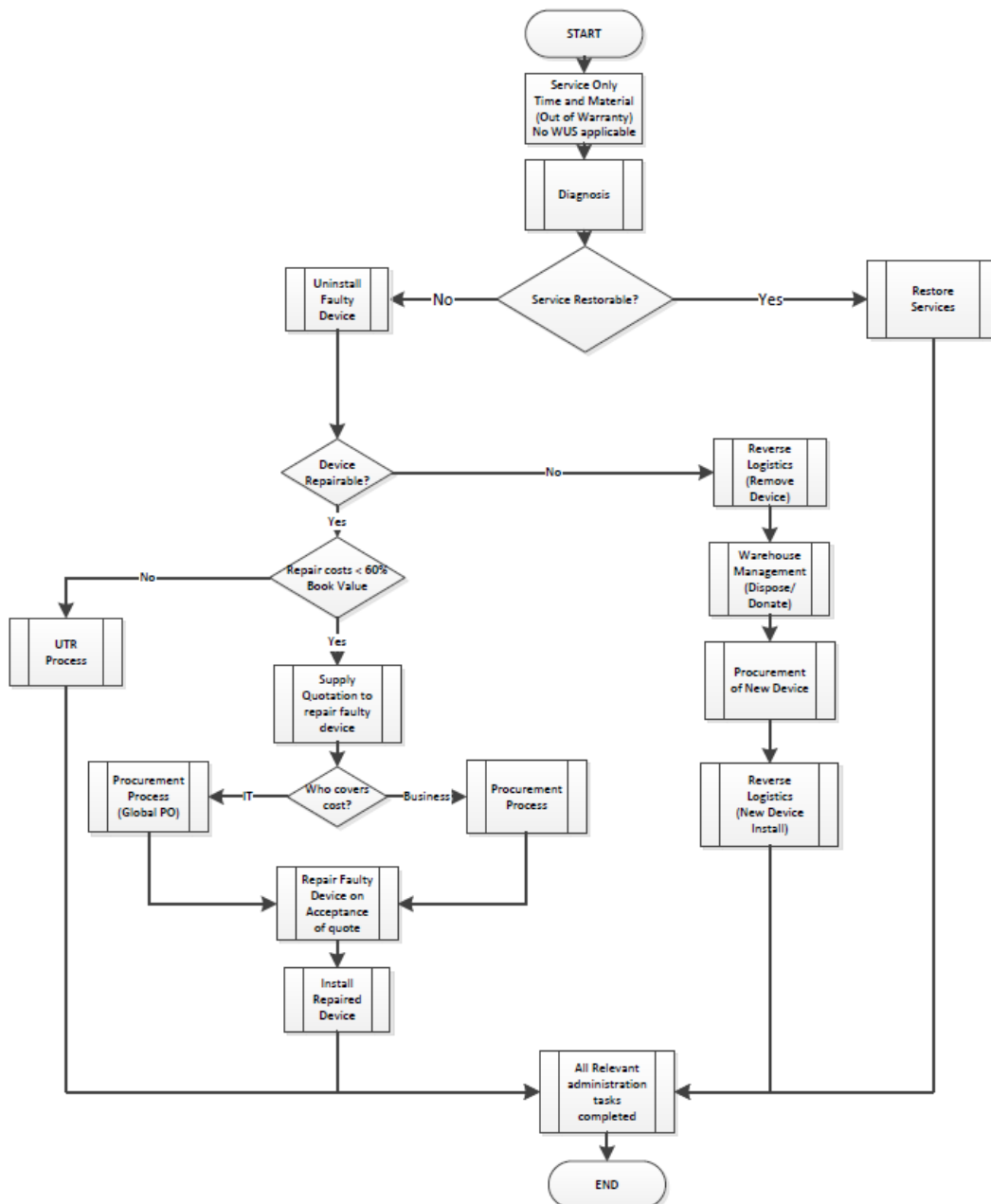


Service Only  
Time and Material  
( Out of Warranty)  
Whole Unit Spares  
applicable

Diagram 5.1 Service Only Time and Material (out of warranty)

## 6 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.



Service Only  
Time and Material  
( Out of Warranty)  
No Whole Unit Spares  
applicable

Diagram 6.1 Service Only Time and Material (out of warranty)

## 7 SERVICE PROVIDER-PROVIDED WUS PROCESS

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

### Service Provider Whole Unit Spares

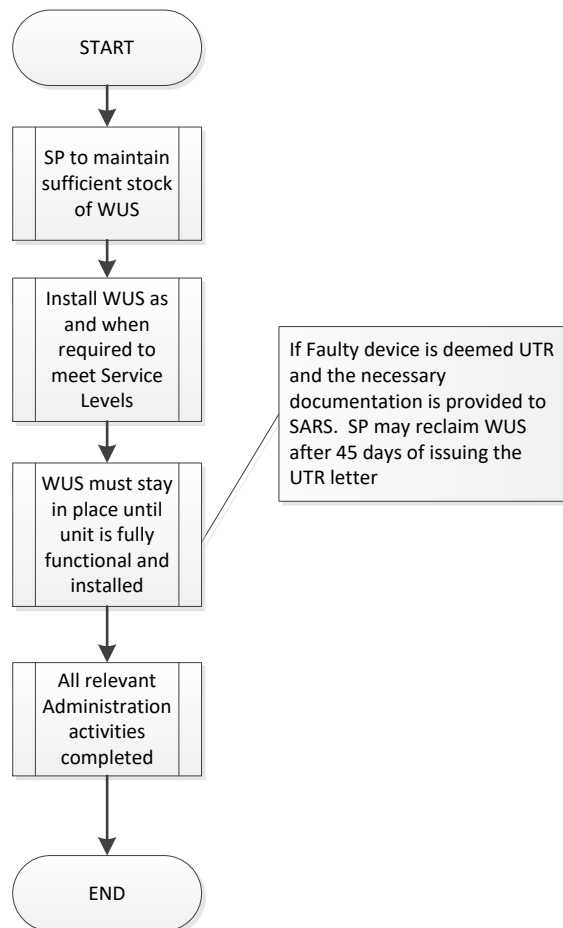


Diagram 7.1 Service Provider (WUS)

## 8 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.

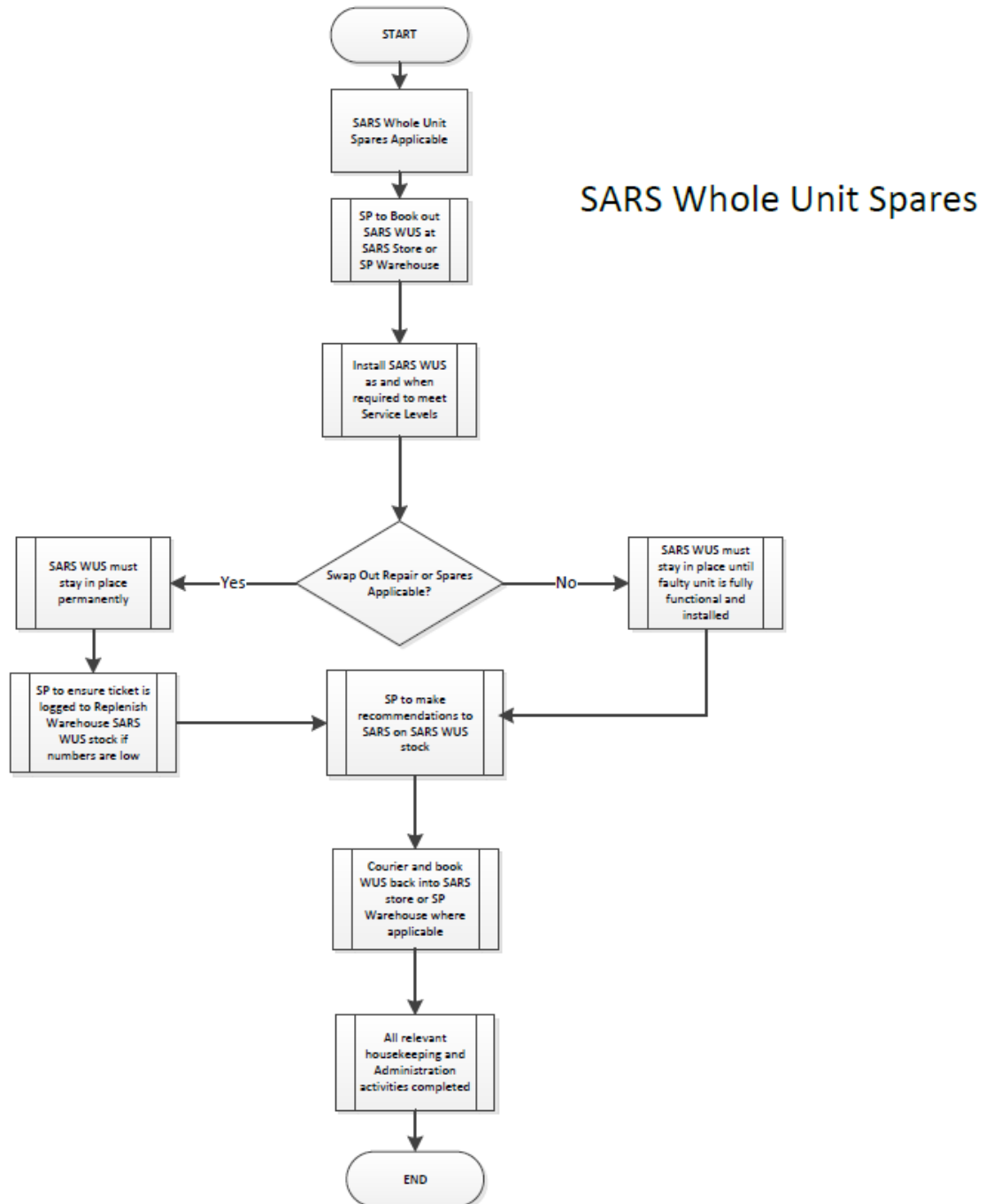


Diagram 8.1 SARS Provided WUS Process

## 9 PRE-PRODUCTION PREPARATION/STAGING PROCESS

The flowchart set out immediately below describes the process to be followed for the pre-production preparation/staging of devices. This process is referred to in the process descriptions that follow. This service is to be rendered as a Standard Chargeable Service.

### Pre Prod Preparation / Staging

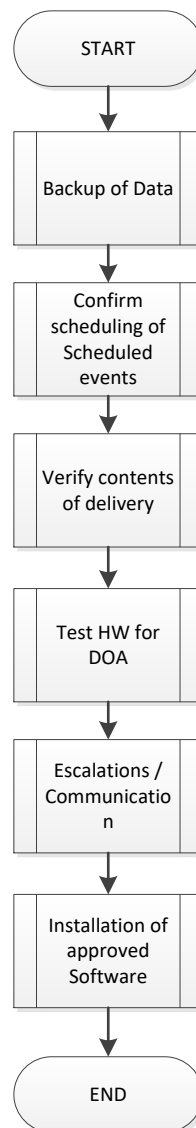


Diagram 9.1 Pre-Prod Preparation/ Staging

## 10 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.

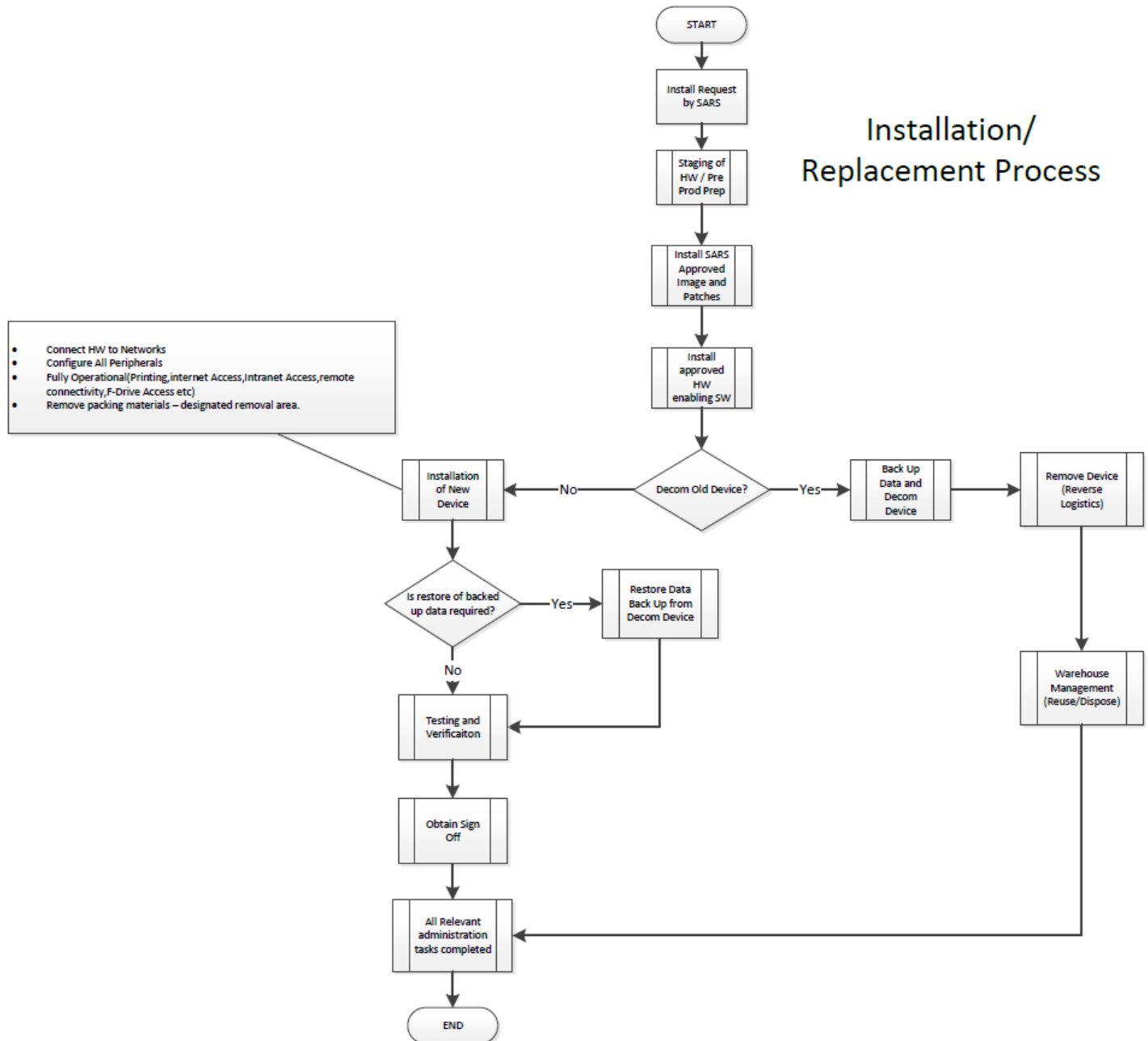


Diagram 10.1 Installation/Replacement Process

## 11 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.

### Move

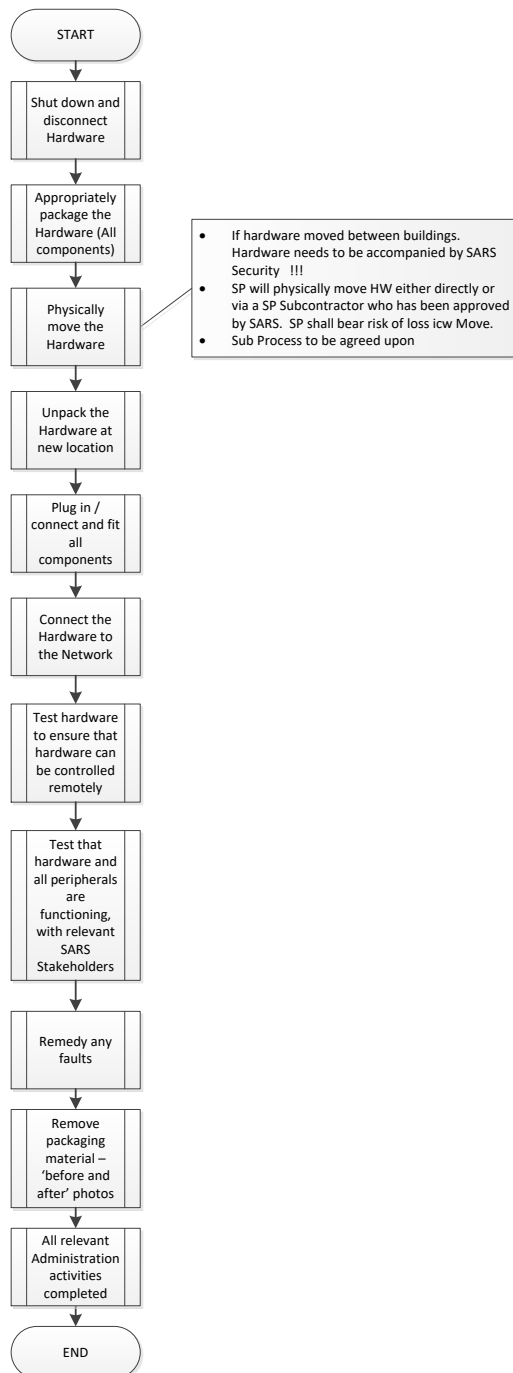


Diagram 11.1 Move Process

## 12 ADD/CHANGE PROCESS

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

### Add / Change

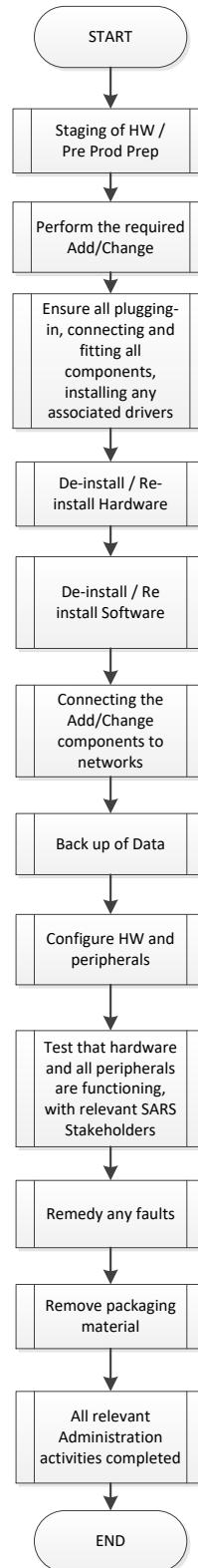


Diagram 12.1 Add/Change



### 13 DECOMMISSIONING FOR RE-USE PROCESS

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

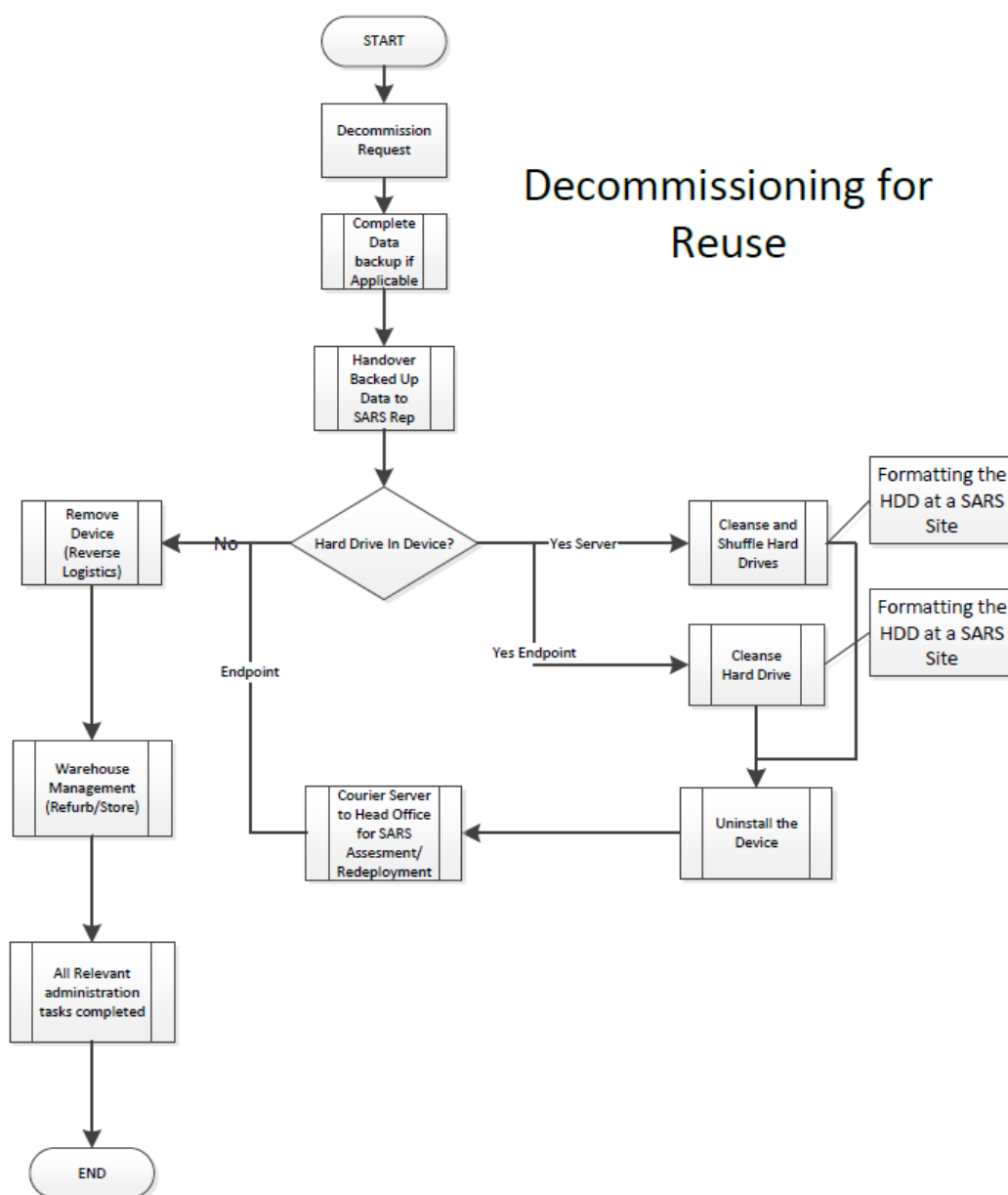


Diagram 13.1 Decommissioning for re-use process

## 14 DECOMMISSIONING FOR DISPOSAL PROCESS

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

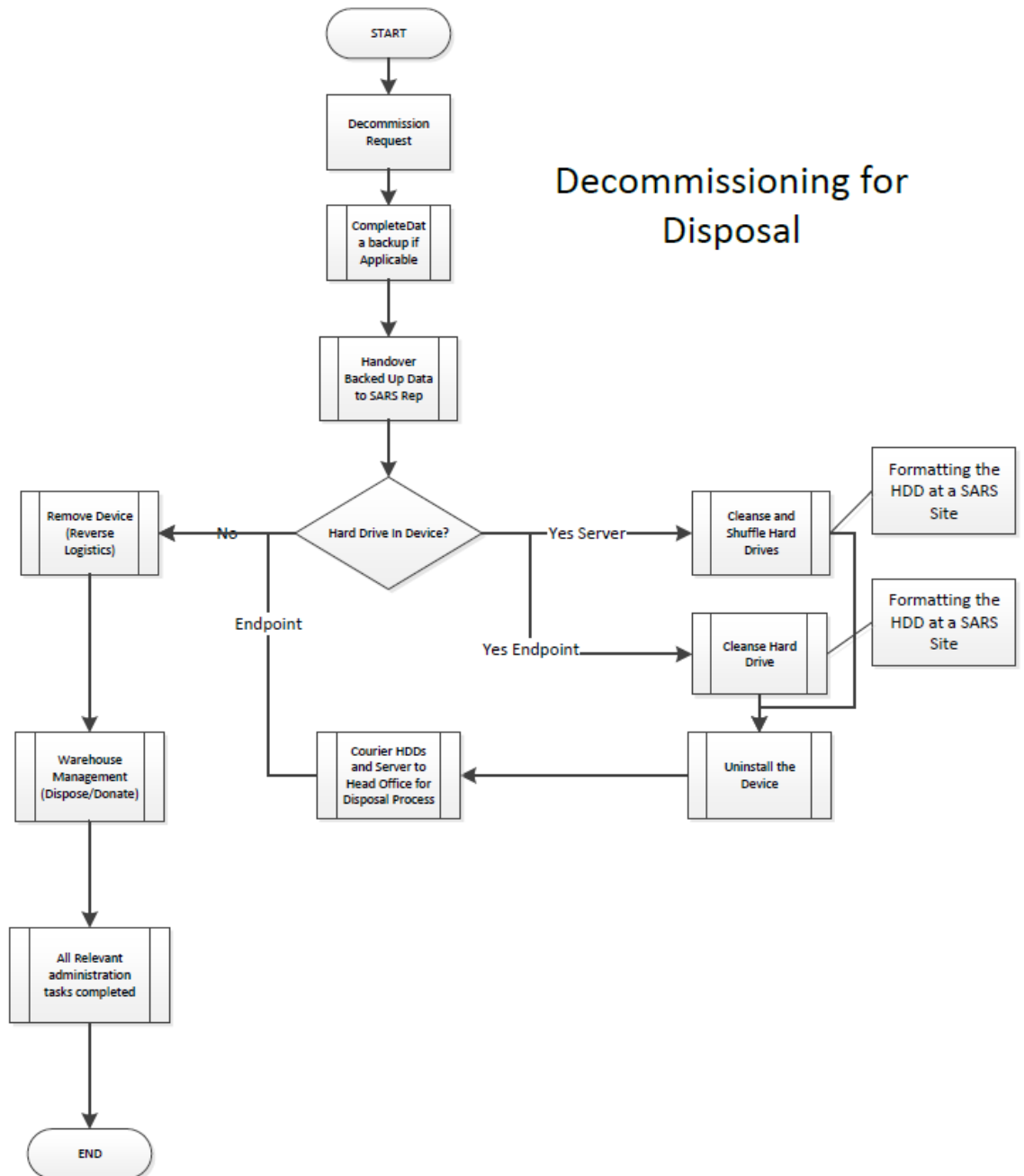


Diagram 14.1 Service Only Time and Material (out of warranty)

## 15 REPAIR PROCESS (END-USER DEVICES)

The flowchart set out immediately below describes the process to be followed for the repair of end-user devices. This service is to be rendered as a Standard Chargeable Service for In-Warranty end-user devices only.

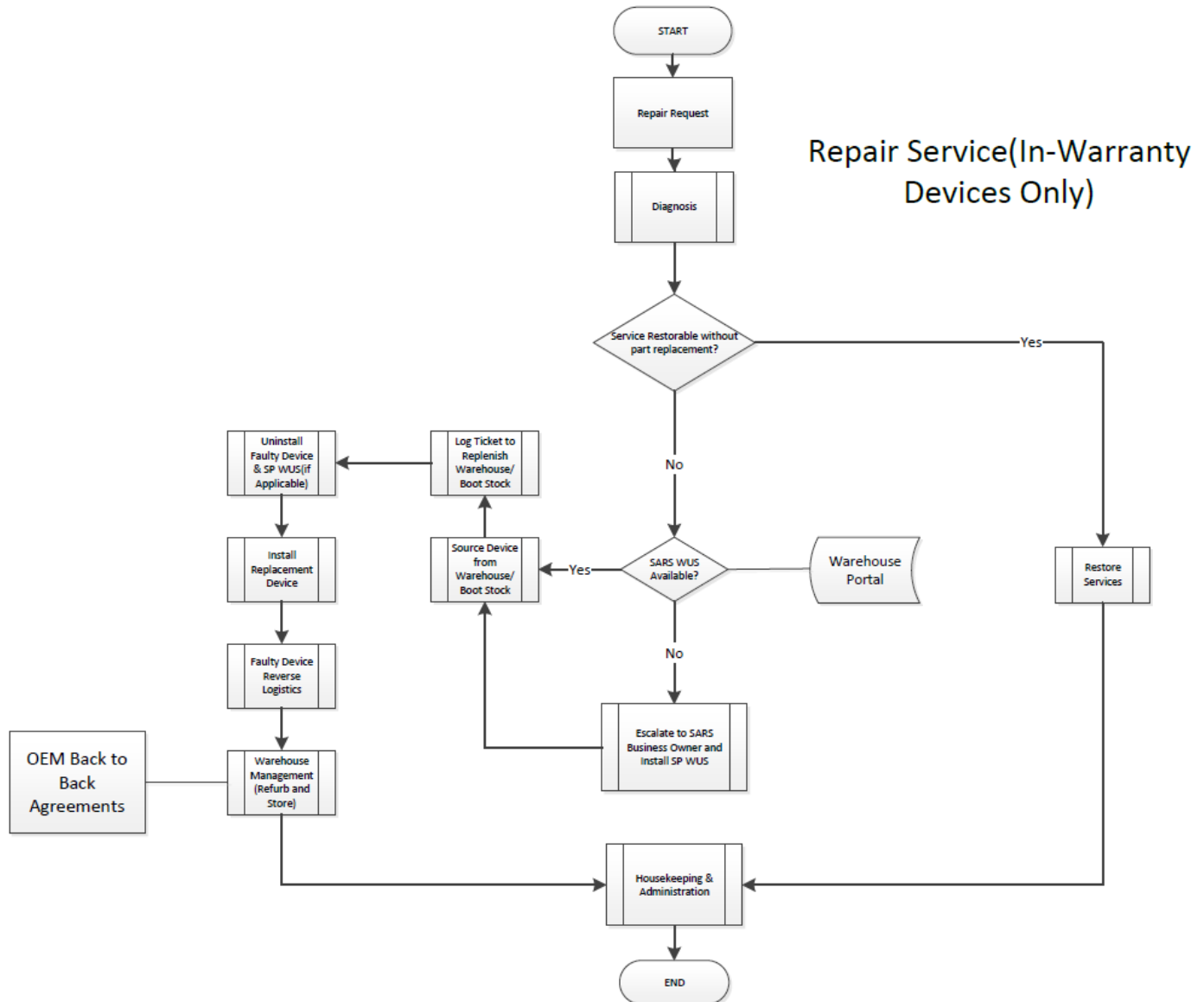


Diagram 15.1 Repair Process (end-user devices: in-warranty only)

**16 INSTALL SERVICE PROVIDER-PROVIDED CONSUMABLE PROCESS**

The flowchart set out immediately below describes the process to be followed for the provision of Service Provider-provided consumables. This service is to be rendered as a Standard Chargeable Service.

### Service Provider Provided Consumables

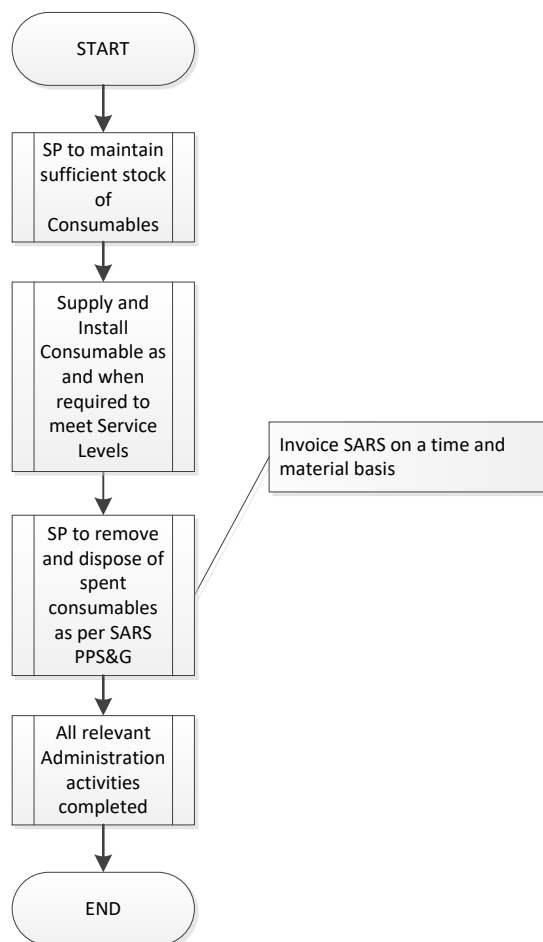


Diagram 16.1 Install Service Provider- Provided Consumables

**17 INSTALL SARS-PROVIDED CONSUMABLES PROCESS**

The flowchart set out immediately below describes the process to be followed for the provision of SARS-provided consumables. This service is to be rendered as a Standard Chargeable Service.

## SARS Provided Consumables

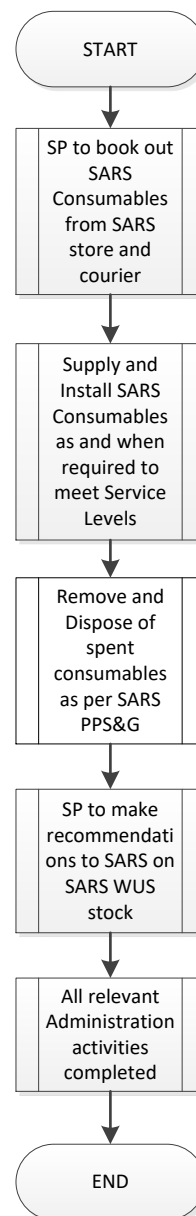


Diagram 17.1 Install SARS-provided consumables process

## 18 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.

### Delivery Acceptance Test

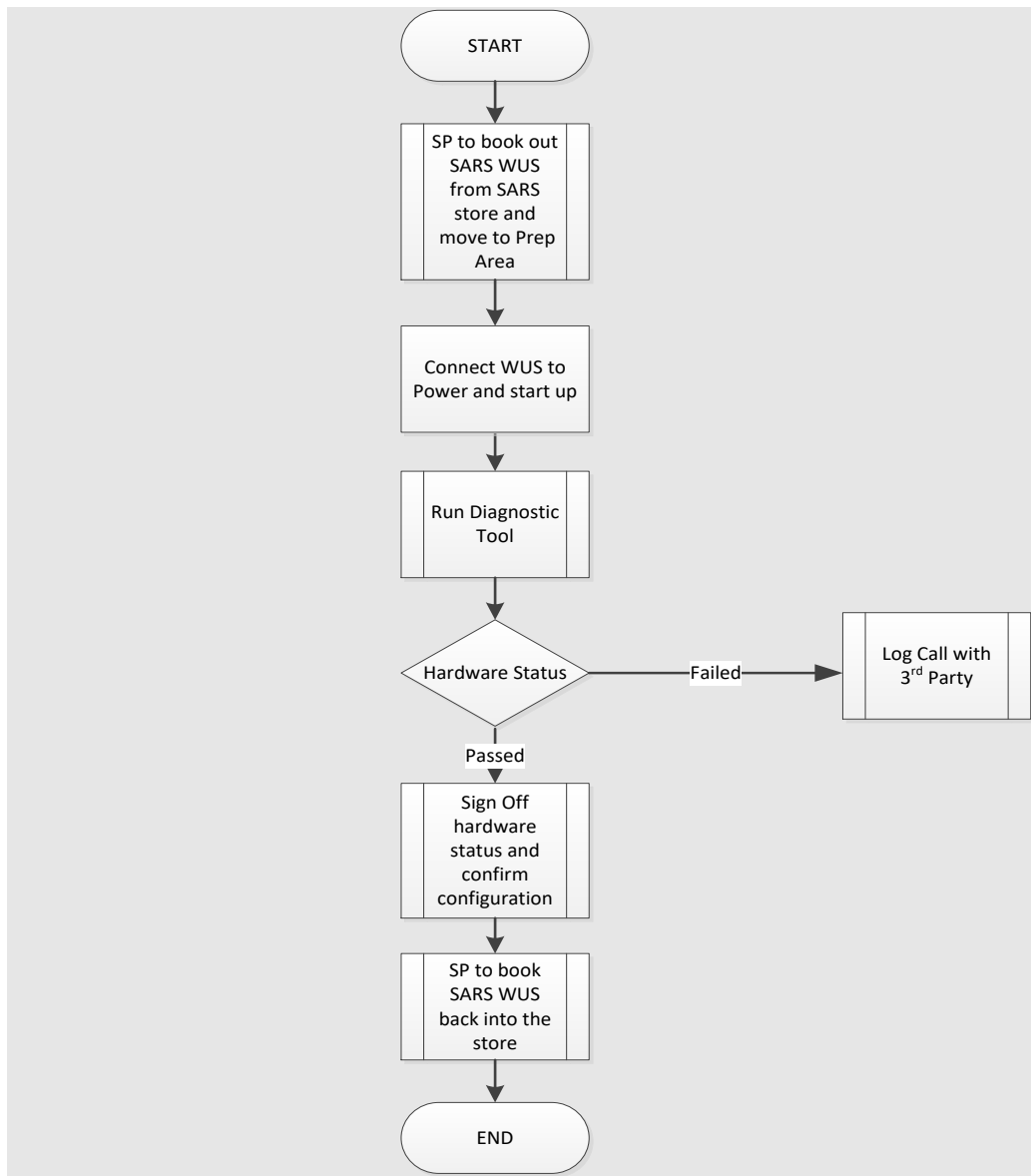


Diagram 18.1 Delivery Acceptance Test

## 19 WAREHOUSE MANAGEMENT PROCESS

The flowchart set out below describes the process to be followed for the management of warehouse services pertaining to device storage, sale, refurbishment, redeployment, and disposal. This service will be rendered as a standard chargeable. This charge will be proportional to the volume of devices actively managed within the warehouse.

Diagram 18.1 Delivery Acceptance Test

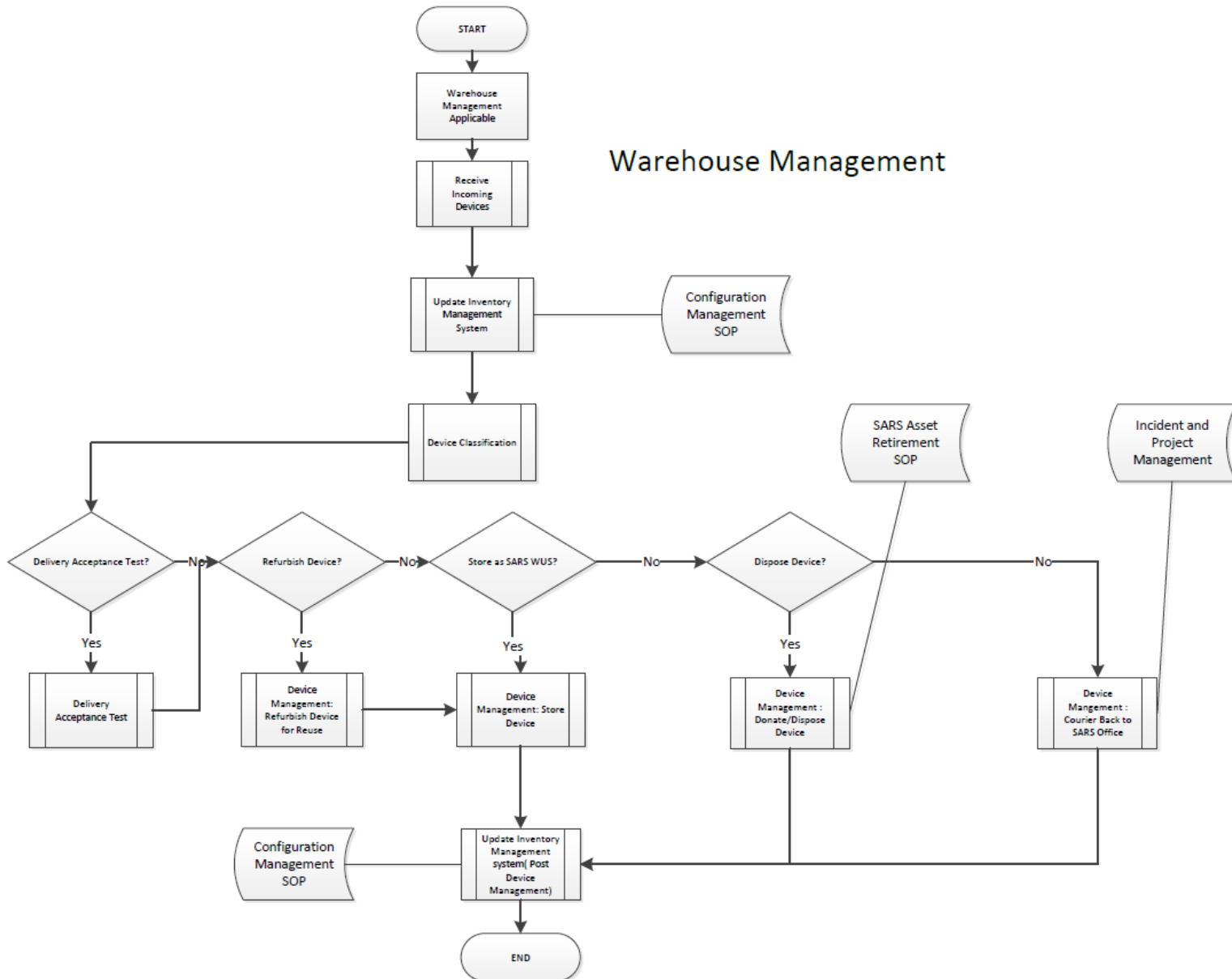


Diagram 19.1 Warehouse Management Process

## 20 REVERSE LOGISTICS PROCESS

The flowchart set out below outlines the process to be followed for the reverse logistics of devices, encompassing the collection, refurbishment, redeployment, or disposal stages. No additional charges are payable by SARS other than the existing monthly charges and this process is designed to complement all above-mentioned processes.

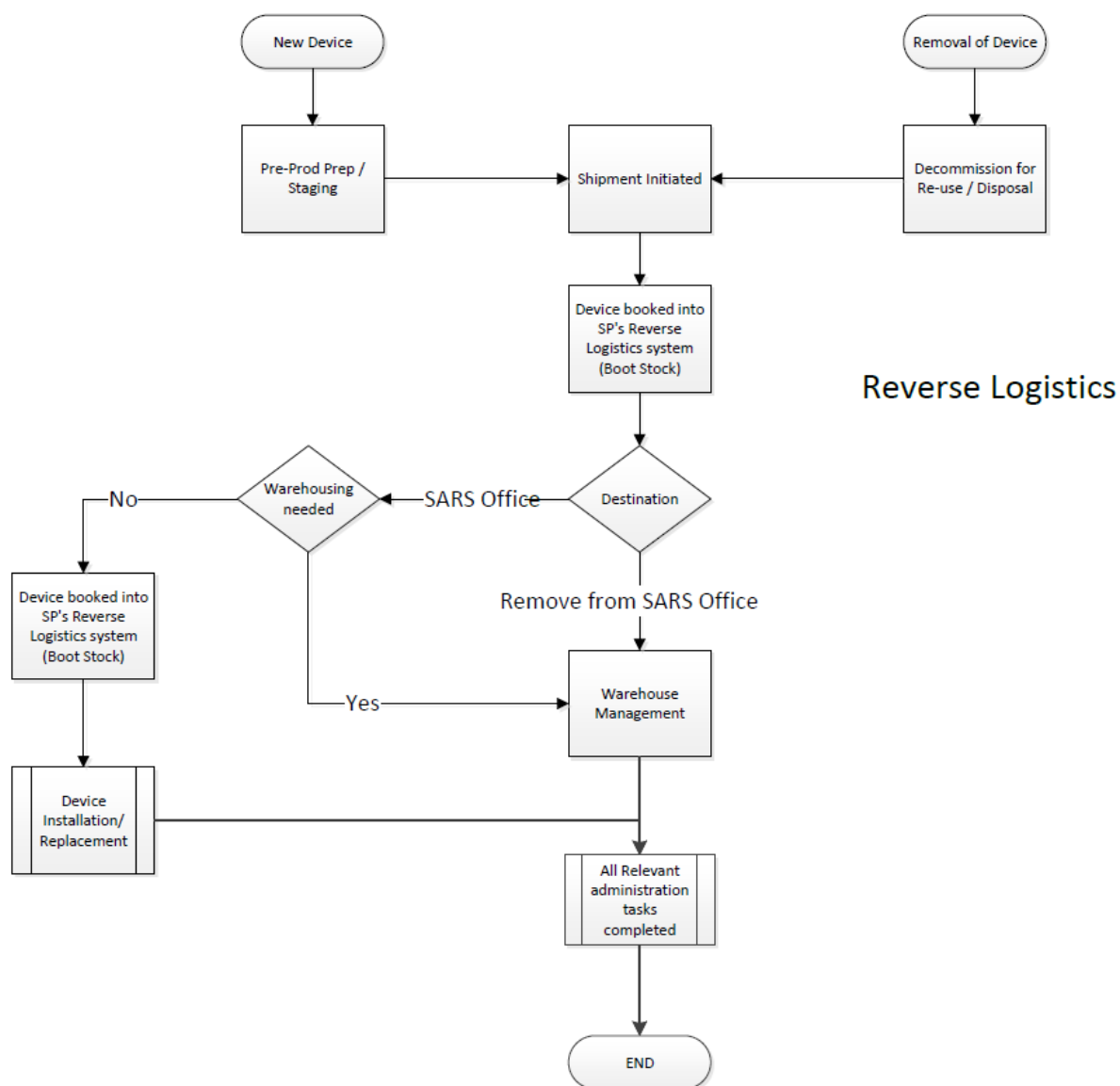


Diagram 20.1 Reverse Logistics Process



## 21 DECOMMISSIONING FOR RE-USE PROCESS (NETWORKS)

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

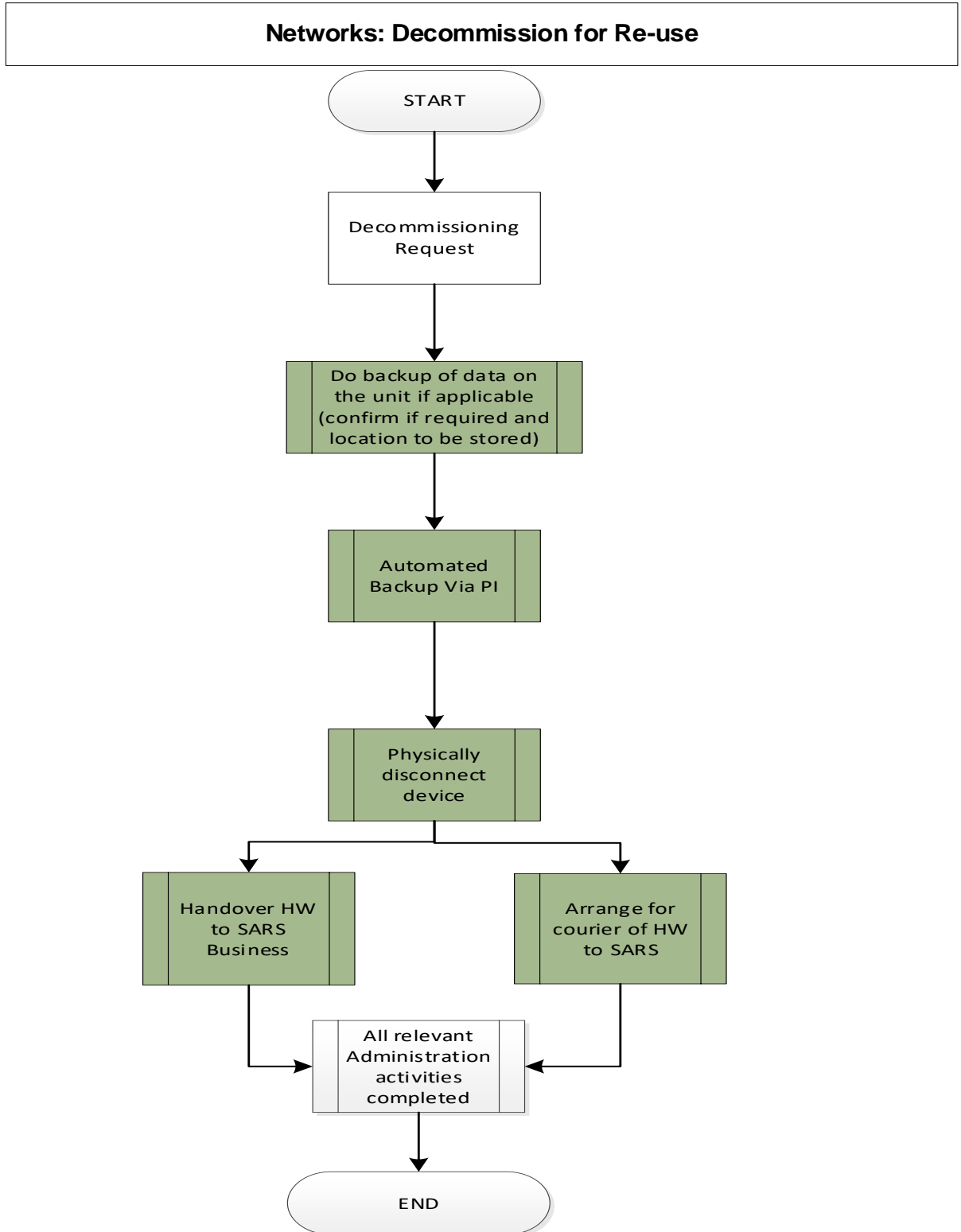


Diagram 21.1 Decommissioning for Re-use Process (Network)

## 22 DECOMMISSIONING FOR RE-USE PROCESS (NETWORKS)

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

### Networks: Decommissioning for Disposal

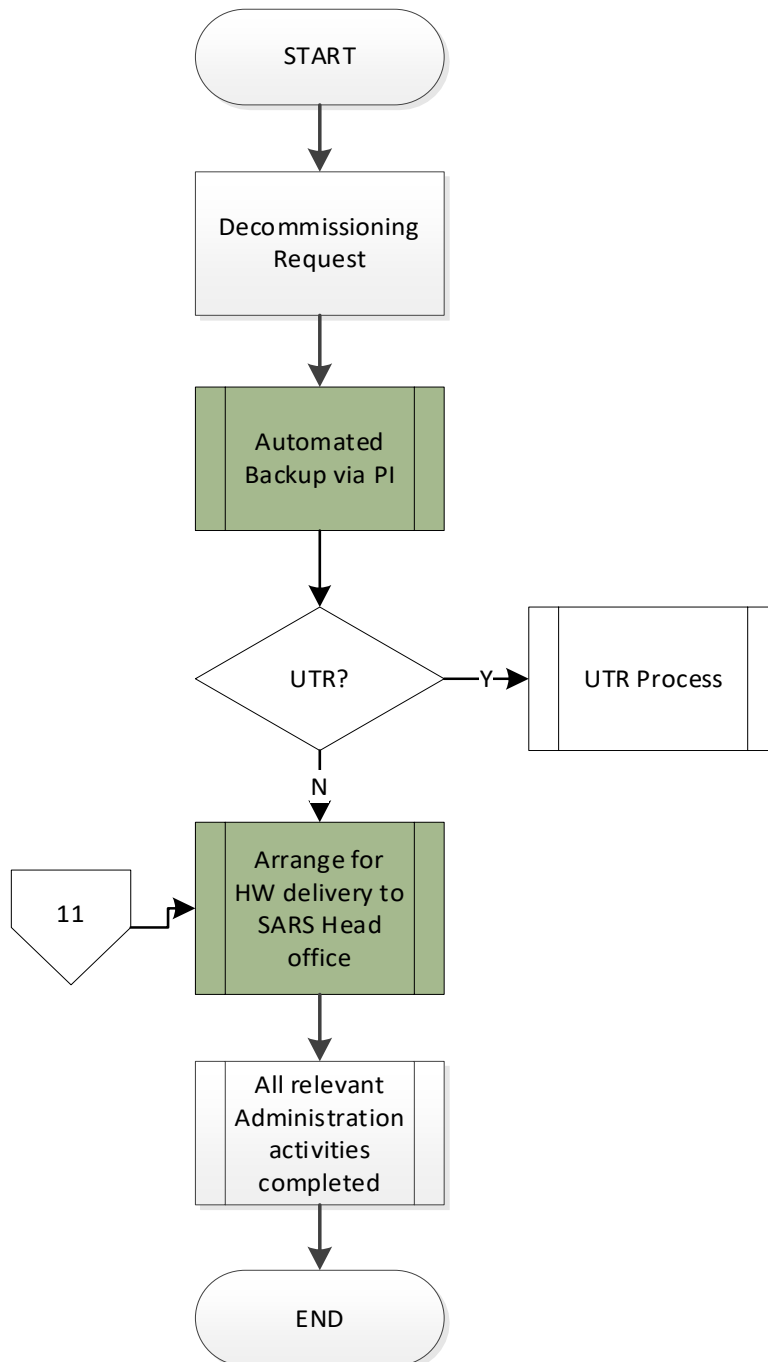


Diagram 22.1 Decommissioning for Disposal