SARS RFP 17/2023

EMPLOYEE CONCIERGE PROGRAMME

Business requirements Specification

Table of Contents

[1 Usage of Terms in this Document 3](#_Toc120872305)

[2 Background 4](#_Toc120872306)

[3 Statement of need\Solution Requirements 6](#_Toc120872307)

[4 Scope of Work7](#_Toc120872308)

[5 deliverables 13](#_Toc120872309)

[6 General Requirements for the services 17](#_Toc120872310)

**Business Requirements Specification**

EMPLOYEE CONCIERGE PROGRAMME

This document forms part of the RFP pack. The document sets out the business requirements for the Employee Concierge Programme.

This document and any appendices must be read in conjunction with all other documents in the RFP pack as such documents 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:

* RFP Main Document
* Technical Evaluation Criteria

1. USAGE OF TERMS IN THIS DOCUMENT
   1. **References to Other Documents in the RFP pack**

Underlined and italicised names are references (or short names) to other documents in the RFP pack. The Bidder must refer to the *RFP Main Document* for the table of documents and their short names (abbreviations / acronyms).

* 1. **Glossary Table**

The capitalised terms in this document appearing in the glossary table below will have their corresponding meanings. The Bidder is referred to the *RFP Main Document* for the use and meaning of capitalised terms generally in the RFP pack.

|  |  |
| --- | --- |
| **Term** | **Meaning** |
| EVP | Employee Value Proposition |
| SAAS, | Software as a service |
| PAAS | Platform as a service |
| IAAS | Infrastructure as a service |
| POPIA | Protection of personal information |
| SLA | Service level agreement |
| CSP | Cloud service provider |
| TLS | Transport Layer Security |

* 1. **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 indicates that it is mandatory) the Bidder must build and price its solution accordingly. If a proposal fails to meet or does not address a mandatory requirement, the proposal may, at SARS’s discretion, be disqualified at any stage of the evaluation process as being non-responsive.

Directory requirements (i.e. where the business requirement, by the context; presence of verbs such as ‘may; ‘should; ‘can’ etc.; or explicit instructions indicate that it is directory) are requirements that SARS does not regard as mandatory.

1. BACKGROUND

The SARS EVP aims to provide a flexible, agile, and meaningful value proposition that leverages a conducive working environment and continuous career development linked to the purpose that enables our employees to thrive and support the achievement of our vision and strategy. The objective is to leverage economies of scale to provide a flexible, agile, and meaningful value proposition within an environment that yields positive employee experiences, as this will ensure that SARS continues to attract and retain the best talent in the future and align the EVP to the changing world of work, and holistic employee expectations.

In the new world of work characterized by digitalization, automation, the Internet of Things, and the on-demand economy SARS is committed to continuing to enhance the employee value proposition and better the quality work/life balance of its employees. The reality is that the latest technologies and workplace expectations are blurring the line between work and life. With our employees having to deal with the pressures of long working hours and hectic lifestyles, the impact of these everyday stresses on the well-being of employees and their families is becoming imperative to recognize and address.

SARS is procuring the services of an employee concierge programme to give employees customized assistance through a range of services, including taking care of personal errands, travel planning, event coordination, reservations, and other lifestyle responsibilities. The objective is to simplify and enhance employee lifestyles by providing access to value-added services that take care of lifestyle tasks and needs that will save employees time, money, and effort whilst balancing work deliverables. The service includes access through a mobile application or website, with multifactor authentication that is available 24/7 with secure in-app payment.

1. Statement of need\Solution Requirements
   1. **Business need**

Our workforce is multicultural, multi-generational, and multi-location. Lifestyle benefits promote an inclusive organizational culture. Through customizing the benefits to address all the needs of the diverse workforce, SARS intent to prioritize and create an inclusive workplace for all employees. For example, assisting employees living with disability to obtain their monthly chronic medication, or supporting parents with school-going children with tutoring services. Employee Lifestyle programs, particularly in the form of flexible benefits, are ideal for personalization and inclusivity.

Through this program, SARS wants to offer employees a competitive and differentiated value proposition that distinguishes SARS from talent competitors among current and future talent.

In this current socio-economic climate and fast-evolving workplace conditions, procuring and introducing a program that is customized for employee needs are hugely beneficial to increase employee engagement and retention in the future.

* 1. **SCOPE OF WORK**

The services provided through the programme will include the following:

* + 1. **Errand Running:** Completing various errands like picking up and delivering medical prescriptions, dry cleaning, license renewals, home affairs documents, post office queuing, or mailing packages within 24 to 48 hours depending on the specific tasks.
    2. **Personal Shopping:** The goal of these personal shopping services is to simplify the shopping process, save time, and help employees make well-informed purchasing decisions either online or in physical stores. These services cater to various shopping needs and preferences and provide employees with discount offerings:
  + Grocery and Household Shopping: Creating grocery lists, purchasing groceries and household essentials, and arranging for same-day delivery or pickup.
  + Technology and Electronics: Recommending and purchasing electronics, gadgets, or tech accessories based on specific needs and preferences.
  + Clothing and Fashion: Assisting with shopping for clothing, accessories, and footwear, including selecting outfits for specific occasions or seasons within the timeline and budgetary requirements.
  + Gift Shopping: Finding and selecting thoughtful gifts for birthdays, holidays, anniversaries, or special occasions, and handling gift wrapping and delivery within a 24-hour turnaround time.
  + Meal Delivery: Assisting with information on nutritious meal delivery services tailored to dietary needs and preferences within a 24-hour turnaround time.
  + Personal Shopping Research: Conducting research on specific products or services to provide recommendations, price comparisons, and reviews.
  + Returns and Exchanges: Handling returns, exchanges, or refunds for items that may not meet expectations.
  + Online Shopping Assistance: Helping individuals navigate online shopping platforms, compare products, and make secure online purchases. Offer special discount rates for SARS employees at major supermarket chains.
    1. **Childcare:** These services are designed to support working parents by taking care of various aspects of childcare; allowing them to focus on their professional responsibilities with peace of mind. The services should include:
  + All employees who are parents of school going children (Grades R to 12) will have access to a homework helpline that assists all pupils with assignments in all major South African languages.
  + After-School Care: help find service providers that can assist employees with Au pair services that will provide after-school care, transportation from school to activities or home, and supervision until parents are available at a reduced rate for SARS employees.
  + Parent-Teacher Meeting Support: Coordinating schedules and reminders for parent-teacher meetings and helping parents prepare for these meetings.
  + Birthday Party Planning: help find party venues, party supplies and event coordinators to assist working parents to organize and plan birthday parties or special events for children, at reduced rates.
  + Childcare Resource Referrals: Providing information on local childcare providers, daycare centers, and babysitting resources for parents within 24 hours.
  + School Enrolment Assistance: Assisting parents in the enrolment process when enrolling their child in a new school or program.
    1. **Senior care** options: Helping employees manage the well-being and care of elderly family members. These services aim to provide support, convenience, and peace of mind to employees who are responsible for the care of seniors in their families. The response time for assisting employees with information about service providers, within a budget range and specific location, is expected within 24 hours of request. The services include:
  + Finding reliable elder care providers assisting with daycare arrangements or helping with senior care options.
  + Assisted Living Placement: Assisting employees in finding suitable assisted living facilities or nursing homes for their elderly relatives, considering factors like location, amenities, and affordability.
  + Home Care Services: assisting employees in finding information on service providers related to in-home caregivers who can help with daily activities, medication management, and companionship for seniors who prefer to stay in their homes.
  + Meal Delivery: Finding nutritious meal delivery services tailored to dietary needs and preferences.
    1. **Travel and Event Planning**: Concierge services to assist with planning vacations, booking flights and accommodation, and organizing events or special occasions, such as birthdays or anniversaries. Employees can speak to dedicated travel agents who can not only negotiate exceptional deals on accommodation and transport, but can also schedule visa meetings, provide inoculation information, and arrange activities for the holiday. Basically, employees only have to phone, say where they want to go (nationally or internationally), and pack their bags. The request for information is within 24 hours and for booking/confirmation of services such as flights, hotels, transportation, and events with a turnaround time of 24-48 hours.
    2. **Pet Services:** Assisting employees with pet care, such as finding pet sitters, grooming services, or arranging veterinary appointments. The objective is to support by making it easier to care for their pets while managing their work and personal lives. The response time for a request for information is within 24 hours. The pet services include:
  + Pet Sitting: Assist employees in finding experienced pet sitters to care for pets when employees are away from home, including feeding, exercise, and companionship.
  + Dog Walking: Scheduling regular dog walking services to ensure dogs get the exercise and outdoor time they need to keep them physically and mentally stimulated.
  + Pet Boarding: Finding and booking reputable pet boarding facilities for employees' pets when they need to travel.
  + Pet Transportation: Arranging transportation for pets to and from the veterinarian, grooming appointments, or other destinations.
  + Grooming Services: Booking grooming appointments for pets and arranging for groomers to come to the employee's home if available.
  + Veterinary Appointments: Coordinating and scheduling vet visits for regular check-ups or medical concerns.
  + Pet Supplies: Assisting in purchasing pet food, supplies, and medications, and delivering them to the employee's home.
  + Pet Training: Finding and scheduling pet training sessions or classes to address behaviour issues or improve obedience.
  + Emergency Pet Care: Providing access to emergency pet care services in case of illness or injury.
  + Pet Adoption Assistance: Offering information and resources on pet adoption, including helping employees find local animal shelters and rescue organizations.
  + Pet-Friendly Travel Planning: Assisting in providing information about pet-friendly accommodation and travel arrangements when employees wish to travel with their pets.
  + Pet Insurance Information: Providing information and recommendations on pet insurance options to help employees protect their pets' health.
  + All requests for information within a turnaround time of 24 hours and assistance with bookings within 48 hours.
    1. **Home Services:** These services include such as home repairs, cleaning services, lawn care, or finding contractors for home renovations. The nature of the service is to assist employees in obtaining relevant service providers, based on location and affordability to assist with the following:
  + House Cleaning: Obtain information and assist with scheduling regular or once-off house cleaning services to keep the home tidy and organized.
  + Home Repairs and Maintenance: Obtain information and assist with scheduling of home repairs, maintenance tasks, and renovations, such as plumbing, electrical work, or painting.
  + Lawn and Garden Care: Obtain information and assist with scheduling lawn mowing, landscaping, and gardening services to maintain the exterior of the home.
  + Appliance Repair: Arranging appliance repair or maintenance services for household appliances such as refrigerators, washing machines, or ovens.
  + Pest Control: Obtain information and assist with scheduling pest control services to address infestations or prevent pest problems.
  + Home Security: Obtain information and assist with scheduling of appointments for setting up and maintaining home security systems, including alarm monitoring and surveillance cameras.
  + Home Organization: Obtain information and assist with scheduling appointments with resources to assist with decluttering, organizing, and optimizing living spaces for better functionality.
  + Moving Services: Coordinating professional movers and packing services when employees are relocating.
  + Real Estate Services: Assisting in finding realtors and property listings. Arranging for home inspections when buying or selling a property.
  + Interior Design and Decor: Offering guidance and resources for interior design, furniture selection, and home decor.
  + Smart Home Setup: Setting up and configuring smart home devices and automation systems for convenience and security.
  + Emergency Services: Providing access to emergency home repair or locksmith services for urgent situations with an expected turnaround time of two hours.
  + Requesting information regarding home services like repairs or cleaning is expected within 24 hours, and if assistance is needed to set up appointments, it is expected to be within 48 hours. The service providers will be paid for services delivered by the employees.
    1. **Events Tickets:** Acquiring tickets for concerts, shows, or sporting events be done within 24 – 48 hours of the requests.
    2. **Reservations:** Assistance with restaurant reservations or movies to be done on the same day, depending on availability. Offer special discounts on movie tickets and refreshments.
    3. **Online Shopping:** Assisting employees with online purchases, including selecting products, making secure payments, and arranging for delivery. These services aim to streamline financial transactions, reduce the administrative burden, and enhance financial security for online transactions.
  1. **Collection and Delivery of Concierge Services**

SARS has offices and employees across South Africa’s rural and urban towns/cities including outlying border posts **(Annexure A).** Service provider must have their own delivery infrastructure and be able to deliver to all SARS locations.In remote locations, service provider may negotiate (subcontract) with local services providers i.e courier services companies to reach SARS offices. Depending on the number of employees at the SARS location, deliveries and pickup services may be done once or twice a week. Employees will have the option to choose their collection or delivery point which can be home or nearest SARS office.

* 1. **Technology Requirements**

SARS require an online tun-key solution; available 24/7/365 and is easy to use. Includes a web-interface and a mobile application that are in line with Legislative requirements, Standards and International best practices as stipulated in this requirement specification. Subscription levels should be scalable up and down according to demand. The requirements are to be commercially available based on the following conditions:

* General services: Mondays to Fridays from 7 am to 7 pm and Saturdays from 8 am to 1 pm.
* Emergency services e.g., Emergency Services: Providing access to emergency home repair or locksmith services for urgent situations with an expected turnaround time of two hours: Available 24/7.
* Critical downtimes (maintenance) must be communicated upfront and where/when services might not be available.
  + 1. **Security Requirements**

SARS require the Service Provider to stipulate whether the components comprising the Service Provider’s solution will be hosted within Service Provider’s own Data Centre, and/or, within a public cloud service. Also, if any component of the Service Provider’s solution makes use of a cloud (SAAS, PAAS, IAAS) service. This should be clearly indicated and described.

3.4.2 **Service Provider Personnel Security**

The Service Provider will be required to provide details of the Service Provider’s screening and vetting processes of the Service Provider personnel and will ensure that all Service Provider personnel complete the SARS Oath / Affirmation of Secrecy. After terminating the employment of any Service Provider Personnel or transferring such personnel from the SARS account to other work, the Service Provider will eliminate any risk from the Services by, amongst other actions, denying such personnel access to any part of the environment from which the Services are provided to SARS and to inform SARS of such. Service Provider will ensure that the Service Provider Personnel are suitably trained and certified to be able to comply with all information security standards, procedures and best practices set out in this Requirement.

3.4.3 **Data Protection and Confidentiality**

The Service Provider will not utilise any SARS Data and/or personal information as defined in POPIA of any SARS employee/s for any purpose other than that of providing the Services under this Requirement. The Service Provider will not possess or assert any lien or other right against or to SARS Data. No SARS Data and/or personal information as defined in POPIA of any SARS employee/s, or any part thereof, will be sold, assigned, leased, or otherwise disposed of to Third Parties by the Service Provider or commercially exploited by or on behalf of the Service Provider, its employees or agents. SARS may at any time on written request to the Service Provider require that the Service Provider immediately return to the SARS or destroy any SARS Data and/or personal information as defined in POPIA of any SARS employee/s and may, in addition, require that the Service Provider furnish a written certification to the effect that upon such return it has not retained in its possession or under its control, either directly or indirectly, any such SARS Data or material and/or personal information as defined in POPIA of any SARS employee/s. The Service Provider will implement on or before the Effective Date, and thereafter maintain, appropriate safeguards against the unauthorised access to, and destruction, loss, or alteration of, the SARS Data and/or personal information as defined in POPIA of any SARS employee/s in the Service Provider’s possession which safeguards are: (i) acceptable to SARS, and (ii) no less rigorous than the most rigorous of the practices maintained by SARS or the Service Provider as of the Effective Date. The Service Provider will during its execution of the Services, engage with 3Rd Parties, and during such engagements, acknowledges the great importance of the Confidential Information to the Disclosing 3rd Party and, where applicable, Third Party proprietors of such information, recognises that the Disclosing Party and/or Third Party proprietors may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Requirement. In this regard each Party will maintain the confidentiality of the other Party’s Confidential Information, using at least the same efforts as it uses to maintain the confidentiality of its own Confidential Information, and as otherwise required under applicable law (POPIA), the terms of this Requirement and the SARS Oath of Secrecy.

The Service Provider will not disclose or publish any Confidential Information in any manner, for any reason or purpose whatsoever without the prior written consent of SARS and provided that in the event of the Confidential Information being proprietary to a Third Party, it will also be incumbent on the Receiving Party to obtain the consent of such Third Party. The Service Provider not to utilise, employ, exploit or in any other manner whatsoever use the Confidential Information for any purpose whatsoever without the prior written consent of the Disclosing Party and provided that in the event of the Confidential Information being proprietary to a Third Party, it will also be incumbent on the Receiving Party to obtain the consent of such Third Party. The Service Provider will restrict the dissemination of the SARS Confidential Information and/or personal information as defined in POPIA of any SARS employee/s to only those of its Staff members who are actively involved in activities for which use of Confidential Information is authorised and then only on a "need to know" and “least-privilege” basis and the Receiving Party will reasonably initiate, maintain and monitor internal security procedures to prevent unauthorised disclosure by its Staff prior to giving any Staff, access to any Confidential Information; and to take all practical steps, both before and after disclosure, to impress upon its Staff who are given access to SARS Confidential Information and/or personal information as defined in POPIA of any SARS employee/s, the secret and confidential nature thereof. The Receiving Party will protect the Confidential Information in the manner, and with the endeavour, of a reasonable person protecting their own Confidential Information. In no event will the Receiving Party use less than reasonable efforts to protect the confidentiality of the Confidential Information.

3.4.4 **Intellectual Property Rights**

SARS retains all right, title and interest in and to the SARS Intellectual Property, including the SARS Intellectual Property that is used in connection with Services or incorporated into any deliverable hereunder, as well as any Intellectual Property developed specifically for SARS by the Service Provider for purposes of providing the Services. With respect to Third Party Intellectual Property that is Commercial Software, the Service Provider will consult with SARS before implementing any Commercial Software and the Service Provider will ensure that it has obtained the necessary permission from the relevant Third Party to use such Commercial Software and to make it available to SARS. Such consultation will specifically address, among other things, SARS options and costs at expiration or termination. The Service Provider's rights to implement such Commercial Software will be subject to the Service Provider's obligations in respect of change control. With respect to Third Party Intellectual Property that is Commercial Software, the Service Provider will consult with SARS before implementing any Commercial Software. Such consultation will specifically address, among other things, SARS options and costs at expiration or termination. The Service Provider's rights to implement such Commercial Software will be subject to the Service Provider's obligations in respect of change control.

3.4.5 **Data residency**

SARS require the Service Provider to indicate whether the Service Provider Services are in part of in whole offered through a Cloud Provider Service. Should the Services or part thereof be provided through a Cloud Provider, SARS prefer such Cloud Services be rendered from within the borders of South Africa. Data residency is of critical importance to SARS and therefore should reside within the borders of the Republic of South Africa. Should the Service Provider provide such Cloud Services outside of the Borders of South Africa, the Cloud Service Provider must comply with relevant laws, such as section 72 of the POPIA, SARS must understand to which legal jurisdictions SARS’s data will reside, once that understanding is established, Service Provider should ensure alignment with POPIA, The Service Provider must ensure their service-level agreements (SLAs) with Cloud Service Providers are established and these must be shared with SARS.

3.4.6 **Data Sovereignty**

The Service Provider must ensure that the legal jurisdictions within which the cloud service provider (CSP) operates are acceptable and not contrary to the laws of the Republic of South Africa. SARS must ensure that the legal jurisdictions within which CSP resides are acceptable and not contrary to the laws of the Republic of South Africa.

3.4.7 **Data Security**

The Service Provider must ensure that their information security strategies, and Policies comply and align with the ISO/IEC 27000 family of standards. Data security solutions to be provided by the CSP must be commensurate with data classification tracking, protection, and encryption.

3.4.8 **Data Encryption**

SARS will require the Service Provider to utilise International best practices in providing the secure web services, and in this regard would require the use of the latest protocol version of Transport Layer Security (TLS 1.3) as it relates to encryption in-transit of Internet communications. SARS will require the Service Provider to utilise International best practices in providing the secure storage of confidential information by means of encryption at-rest and including Full Disk Encryption (DFE) technologies used. The Service Provider will provide further details of FDE technologies used in relation to server and storage hard drives. SARS desires to use the Service provider’s Key Management Services for the storage of encryption keys as it relates to the services. The Service Provider will be required to provide details of such Encryption Key Management Services (KMS) to ensure compliance to ISO 27000 set of standards and International best practices.

3.4.9 **Data Privacy**

The Service Provider must be aware of its data privacy obligations when transferring data (including personal data) into the CSP environment in accordance with the POPI Act principles of compliance on data privacy. The Service Provider must regularly review privacy of SARS information and a report must be provided to SARS on a quarterly basis. The Service Provider through its CSP, must monitor and ensure that the collection, processing, storage, transmission, use and disposal of information (including personal) occurs in line with the POPI Act & (ECT Act) and According to PAIA requirements on cloud computing. If the privacy of data has potentially or been compromised while in the Service Provider and/or CSP cloud environment, the Service Provider must inform SARS of such incident, such reporting must include details of the nature, extent, and details of data compromised and in according of the provisions of the POPIA, Notification of Security Compromises. The Service Provider must ensure that the contract with the CSP includes clear provisions for the deletion/ disposal/ erasure of data (including personal information). Such deletion or erasure shall be done with SARS authorisation and in a responsible and secure manner by the CSP after consultation and agreement with SARS. SARS will require the CSP provide SARS with a certificate of proof that such data disposal.

3.4.10 **Risk Management**

The Service Provider must undertake a comprehensive risk assessment of all relevant aspects of the Service Provider computing service being provided prior to the commencement of the SARS services. The risk assessment approach should consider or follow the following:

* ISO 31000 Risk management – Principles and guidelines;
* ISO/IEC 27018; and
* Other relevant regulatory requirements, i.e., POPI, Consumer Protection Act (CPA) add other relevant legislation.

The Service Provider must provide third party accreditation of the CSP. The Service Provider must constantly monitor whether the CSP environment is audited annually. The CSP must provide SARS with any areas of non-compliance. SARS require the Service Provide to conduct regular audits of the ICT environment comprising the Services rendered to SARS and to inform SARS of any finding that would affect the confidentiality, integrity availability or privacy of SARS information as it relates to the Services. SARS require the Service Provide to provide details of its processes with regards to patch management and malware protection (anti-virus management) as it relates to the Services. This must be in line with International Standard Organisation (ISO), National Institute of Standards and Technology (NIST) and Original Equipment Manufacturer (OEM) standards of best practices. SARS require the Service Provider to perform regular threat and vulnerability assessments to determine any risks within the provider Services and to implemented mitigation measures to prevent any cyber-attacks from taking place.

* + 1. **Records Management**

The Service Provider must monitor and ensure that records and data created, stored or managed by the CSP remain accessible and retrievable in order to meet all regulatory requirements for information access as required by the POPI Act, PAIA and other legislation.

* + 1. **Contracting**

The Service Provider must ensure the existence of the Cloud Service Level Agreement (Cloud SLAs) to support the contractual relationship with the CSP, where applicable. The Cloud SLA must, where practically possible and applicable, include penalty clauses and some incentives for the parties. The Intellectual Property (IP) of the data in the cloud belongs to the SARS as defined in the contract. The Service Provider must ensure that the CSP is contractually prohibited from using “hosted” SARS data or information for any of the CSP’s advertising or commercial purposes. The Service Provider and CSP must comply and adhere to the laws of the Republic of South Africa and must demonstrate compliance with POPI Act, PAIA, and any other applicable laws.

The Service Provider consents that SARS is the owner of all rights, title, and interest in the data and that all data will be maintained, backed up and secured until returned on termination of the agreement (unless other provisions are made for the migration, transfer, or destruction of the data). The Service Provider will consent that data processing (mining) shall be carried out in a manner provided for by the POPI Act and as authorised by SARS. The Service Provider will provide the actual geographic locations where data storage and processing of SARS data will occur, which must be to SARS’s satisfaction. The Service Provider will provide the jurisdiction which governs the operation of the Cloud SLAs referred to in paragraph 3.4.12 above. Contract, and application of privacy, confidentiality, access, and information management laws.

The Service Provider will ensure that data storage and processing is restricted to the specified locations where the regulatory framework and technical infrastructure were agreed to, and to ensure that the Service Provide maintain adequate controls over the SARS data. The Service Provider must demonstrate compliance, including a warranty in relation to security, related storage, and access obligations, and Service Level Agreement (SLA) referred to in paragraph 3.4.12 above that include cost and operating requirements of providing service continuation in business critical and non-business critical services when disruptions arise. The Service Provider must provide details of the security provisions relating to the service, consistent with the Service Provider Information Security Policy (and where required, compliance with ISO/IEC 27001), and ISO/IEC 27018.

The Service Provider will ensure that unauthorized access, use and or alteration of the SARS data is prohibited. The Service Provider must provide details of the technical mechanisms and procedures in place to support this restriction (e.g. control of user credentials for authentication, data encryption, information dispersal, data separation, and segregation). The Service Provider must provide details of the technical mechanisms and procedures that prevent data loss (e.g.: contractor/organisation responsibilities and routines for backup, failover or redundancy). The Service Provider must provide details of provisions and procedures for backup, restoration of services and disaster recovery. The Service Provider must provide details of all 3rd party network connectivity as it relates to the Service and must provide details of how secure connectivity is maintained as it related to confidentiality integrity and privacy of SARS users and their information, and; the Service Provider must also provide a seamless web interface through which SARS employees can interact with 3rd party Vendors and retailers.

3.4.13 **Cloud Exit Strategy**

SARS require the existence of a planned exit in preparation for an end or termination of the contract with the Service Provider and CSP. The Service Provider needs to confirm compliance with SARS requirements in this regard. SARS retains an immediate and ongoing right of access to all SARS organisational data held by the Service Provider and/or cloud service provider. The Service Provider should confirm access to SARS information during termination of Services and as part of the agreed contract exit plan. The Service Provider must guarantee the accuracy, integrity, and reliability of data to ensure the ongoing availability of the data and maintain control over its retention or disposal. SARS require that the Service Provider make provisions for the safe return/transfer of data should the cloud service provider be the subject of a takeover. The Service Provider will be required at the termination of the agreement, to make provisions for the secure transfer of SARS data as it relates to the services, at no additional cost to SARS. Metadata relating to SARS in relation to the administration of the services must be disposed of by the Service Provider and as authorised by SARS. SARS will require the CSP to provide SARS with a certificate of proof that such data disposal was performed in line with the provisions of ISO 27001 Requirements for Data and Asset Disposal, the provisions of the POPIA, and/or the provisions of the GDPR and/or that of the Service Provider own disposal policy, whichever process is most rigorous and acceptable to SARS.

3.4.14 **Multi-channel Access / Mobile Application**

SARS require the Services to be offered through a secure Internet Web service as well as through a Mobile Application interface. SARS require the Service Provider provide details of how the Web Services are secured in terms of regular (annually) security assessments, (Penetration testing and Code reviews) as well as Threat and Vulnerability (T&VA) tests performed on a weekly basis. SARS require that these security services (Penetration testing, Code reviews and T&VA) be conducted throughout the duration of the contract. SARS require the Service Provider provide SARS with regular security reporting (Monthly) that would include any risks identified as part of the security services defined above and as it relates to the Services. Any critical risks identified will be communicated immediately and not just as part of the monthly report. The Mobile Application must be available for both Android and iOS platforms and downloadable from the relevant Google / Apple Application Stores to ensure a safe and trusted application market place.

* + 1. **Identity And Access Management (IAM)**

IAM is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. The IAM technology controls user access, Single Sign-on (SSO), two factor authentication, multi factor authentication and privilege access management. SARS require the Service Provider provide details of how access control will be managed in relation to user access, SSO, and MFA in terms of performing sensitive transactions. SARS will also require its Human Resource Department to perform administrative duties and would require privilege access for reasons of reporting and management. This privilege access would require strong authentication, and MFA will be a requirement. The Service Provider should provide detail of these user profiling services. The Service Provider must provide details of role-based access control (RBAC) of Service Provider IT administrative Staff in managing the platform as it relates to the Services. The Service Provider must provide details of how access control activities and associated audit trail information is stored, monitored and managed. SARS require that the IAM technology provides for a secure enrolment process that also incorporate MFA technologies. The Service Provider must provide details of such capability and processes as it relates to the Services. The Service Provider must also as part of the provisions of the POPIA, request explicit consent from the SARS employee upon enrolment, and store such provided consent for future reference and in a manner that is legally acceptable.

3.4.16 **Secure payments**

SARS require the Service Provider to provider for a secure payment gateway service as part of the Online Services. This secure payment gateway must be compliant as per the Payment Card Industry Data Security Standard. The Service Provider is required to provide proof of its compliance by providing to SARS the Service Provider’s PCI-DSS Level 1 Certificate.

3.4.17 **Disaster Recovery Plan**

SARS require that the Service Provider has Disaster Recovery and Business Continuity Plans in place as it relates to the Services, which conform to SARS’s requirements. SARS require the Service Provider provide details of such DRP/BCP processes to ensure alignment with the Service Level Agreement referred to in paragraph 3.4.12 above.

* + 1. **Security Monitoring and Automation**

Continued Security Monitoring (CMS) is a threat intelligence approach that automates the monitoring of information security controls, vulnerabilities, and other cyber threats to support organizational risk management decisions. SARS require the Service Provider to provide details of the Service Provider’s capability with regard to security monitoring, incident management and the related control processes and measures implemented (CIRT) in relation to the Services which must conform to SARS’s requirements.

**3.5** **Legislative requirements**

* + Constitution of the Republic of South Africa, 1996.
  + Electronic Communications and Transactions Act, 2002 (Act No.25 of 2002) (ECTA).
  + Regulation against the Interception of Communications Act, 2002 (Act No.70 of 2002) (RICA).
  + Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (PAIA).
  + The Public Finance Management Act, 1999 (Act No. 1 of 1999) (PFMA).
  + National Strategic Intelligence Act, 1994 (Act No.39 of 1994) (NSI).
  + Protective Disclosures Act, 2000 (Act No. 26 of 2000).
  + Protection of Personal Information Act, 2013) (Act No.4 of 2013) (POPIA).
  + Critical Infrastructure Protection Act,2019 (Act No. 8 of 2019).
  + General Data Protection Regulation (EU) 2016/679.

**3.6 International Standards Instruments**

* + Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, IT Governance Institute (2006).
  + Convergence of Enterprise, Security Organisations, The Alliance of Enterprise Security Risk Management (2005).
  + ISO /IEC 27001:2022 – Information Security– Code of Practice for Information Security Management.
  + ISO 9001 – Quality Management.
  + Payment Card Industry Data Security Standard (PCI DSS).
  + National Institute of Standards and Technology (NIST) Standards of Good Practice.