

Bid Number : SAWS-447/25

Appointment of a service provider to provide a cloud-based eSignature solution for a period of three (3) years.

Closing Date and Time: 11 December 2025 @ 11:00

Validity Period: 90 days from closing date of bid

BRIEFING SESSION

Date:	01 December 2025
Time:	10:00
Venue:	Meeting ID: 310 124 093 177 91 Passcode: cf9Ks9ZQ
Compulsory:	Yes

THIS BID WILL CLOSE ELECTRONICALLY ON THE eTENDER PLATFORM WHICH MAKES PROVISION FOR THE ELECTRONIC SUBMISSION OF BIDS

(<https://www.etenders.gov.za/>)

Bidders responding to this bid must ensure that they complete and submit all the documents issued with this bid together with the bidders' response i.e. any additional documentation before the closing time of this bid. Responses received after the closing time will NOT be considered.

ENQUIRIES:

Any clarification required by a bidder regarding the meaning or interpretation of the document or any aspect concerning the submission is to be requested **in writing** from:

SCM: Acquisition Department South African Weather Service Email: bids@weathersa.co.za

Any enquiries relating to this bid must be submitted in writing not later than 5 days prior to the closing date of the bid.

Contents

Invitation to Bid	Annexure A
General Conditions of Contract (GCC)	Annexure B
Bidder's Disclosure.....	Annexure C
Preference points claim form in terms of the Preferential Procurement Regulations 2022 ...	Annexure F
Pricing Schedule	Annexure G
Specifications / Terms of Reference	Annexure H
Guidelines or requirements specified in DPSA Electronic Signature Guidelines	Annexure H1
POPIA Supplier Notice and Consent form.....	Annexure i

**PART A
INVITATION TO BID**

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF SOUTH AFRICAN WEATHER SERVICE

1 SUPPLIER INFORMATION

The following section must be completed by the bidder. Failure to do so may result in the offer being rejected.

NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					
SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		OR	CENTRAL SUPPLIER DATABASE No:	MAAA
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE	TICK APPLICABLE BOX] <input type="checkbox"/> Yes <input type="checkbox"/> No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT		[TICK APPLICABLE BOX] <input type="checkbox"/> Yes <input type="checkbox"/> No
[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE / SWORN AFFIDAVID (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS CLAIMED]					

ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]
QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS			
IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? <input type="checkbox"/> YES <input type="checkbox"/> NO			
DOES THE ENTITY HAVE A BRANCH IN THE RSA? <input type="checkbox"/> YES <input type="checkbox"/> NO			
DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA? <input type="checkbox"/> YES <input type="checkbox"/> NO			
DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA? <input type="checkbox"/> YES <input type="checkbox"/> NO			
IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION? <input type="checkbox"/> YES <input type="checkbox"/> NO			
IF THE ANSWER IS “NO” TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 BELOW.			

PART B TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION

- 1.1 Bids must be delivered by the stipulated time. Late bids will not be accepted for consideration.
- 1.2 **All bids must be submitted on the official forms provided – (not to be re-typed) or in the manner prescribed in the bid document.**
- 1.3 This bid is subject to the Preferential Procurement Policy Framework Act, 2000 and the Preferential Procurement Regulations, 2022, the General Conditions of Contract (GCC) and, if applicable, any other Special Conditions of Contract (SCC).
- 1.4 **The successful bidder will be required to fill in and sign a written contract form (SBD7).**
- 1.5 Bidders are advised to initial all pages of their bid.
- 1.6 **Submission of bids**

THIS BID WILL CLOSE ELECTRONICALLY ON THE eTENDER PLATFORM WHICH MAKES PROVISION FOR THE ELECTRONIC SUBMISSION OF BIDS (<https://www.etenders.gov.za/>)

Bidders responding to this bid must ensure that they complete and submit all the documents issued with this bid together with the bidders' response i.e. any additional documentation before the closing time of this bid. Responses received after the closing time will NOT be considered.

Returnable Documents:

The following documents must be included:

- Invitation to Bid: Annexure A
- General Conditions of Contract: Annexure B
- Bidder's Disclosure: Annexure C
- Preference points claim form in terms of the Preferential Procurement Regulations: Annexure F
- Pricing Schedule and Financial Proposal: Annexure G
- Specifications / Terms of Reference, Annexure H, together with the bidder's response to Annexure H (Technical / Functional Proposal).
- POPIA supplier consent form: Annexure i
- Any other documentation issued with the bid.

The South African Weather Service (SAWS) reserves the right to reject a bid should it not be submitted in the prescribed format.

- 1.7 The South African Weather Service (SAWS) is not bound to accept any of the offers submitted and reserves the right to:
 - 1.7.1 Reject bids that are not according to Specifications / Terms of Reference;

- 1.7.2 Reject bids with incomplete standard bidding documents (SBD's);
- 1.7.3 Request further information from any bidder after the closing date of the bid for clarity purposes;
- 1.7.4 Conduct site inspection/s to verify the infrastructure of bidders before final selection and award;
- 1.7.5 Not to award the bid if the bid price is not market related;
- 1.7.6 Not to award the bid to a bidder whose tax matters have not been declared by the SARS to be in order;
- 1.7.7 Reject a bid if the bidder has committed a proven corrupt or fraudulent act in competing for any contract;
- 1.7.8 Award the bid in totality to one or partially to more than one bidder;
- 1.7.9 Conduct reference / background checks on bidders and / or individuals to, among other things, verify information provided by a bidder, confirm a firm's existence and track record, identify its owners and affiliations or verify an individual's educational and professional credentials.
- 1.8 The South African Weather Service may, prior to award of the bid, cancel the bid if:
 - 1.8.1 Due to changed circumstances, there is no longer a need for the goods or services requested;
 - 1.8.2 Funds are no longer available to cover the total envisaged expenditure;
 - 1.8.3 No acceptable tenders are received;
 - 1.8.4 Due to material irregularities in the tender process.
- 1.9 Any effort or attempt by a bidder to influence the award decision in any matter may result in the rejection of the bid.
- 1.10 Costs incurred by the bidder in respect of attending any briefing / information / site visit / presentation will be borne by the bidder and the South African Weather Service will not be liable to reimburse such costs incurred by the bidder or his/her representative/s.
- 1.11 Cost incurred by the bidder in preparing and submission of any bid proposal will be borne by the bidder and the South African Weather Service will not be liable to reimburse such costs incurred by the bidder or his/her representative/s.
- 1.12 The South African Weather Service shall on receipt of any proposal relating to this bid become the owner thereof and shall not be obliged to return any proposal.
- 1.13 The bidders shall indemnify the South African Weather Service against all third-party claims of infringement of patent, trademark, or industrial design rights arising from the use of the goods or any part thereof by the South African Weather Service.
- 1.14 The South African Weather Service reserves the right to request a bidder's latest audited financial statements prior to the award of the bid in order to ascertain financial stability of the bidder. Failure by a bidder to provide such information upon request may result in the rejection of the bid submitted by the bidder.
- 1.15 Subcontracting: Tenderers or contractors must submit proof of subcontracting between the main tenderer and the subcontractor. Proof of subcontracting arrangement may include a subcontracting agreement between the main tenderer and the subcontractor.

- 1.16 The SAWS reserves the right to request final presentation only to the short listed bidders to the evaluation committee. The shortlisted service providers will be subjected to present their service offering in line with the bid requirements/scope of work. The SAWS might also conduct site visit to ensure the firm existence and validate the firm’s proposed capacity/employees and administration office.
- 1.17 The service provider must have duly approved operational premises with the necessary infrastructure to provide services and relevant accreditation by the relevant body. Before the awarding of the tender a due diligence site visit will be carried out at the premises of the service provider.
- 1.18 Supplier Performance Management is viewed by the SAWS as critical component in ensuring value for money acquisition and good supplier relations between the SAWS and all its suppliers. The successful bidders shall upon receipt of written notification of an award, be required to conclude a SLA with the SAWS, which will form an integral part of the supply agreement. The SLA will serve as a tool to measure, monitor and assess the supplier’s performance level and ensure effective delivery of service, quality and value-add to SAWS’s business. Successful bidders are required to comply with the above condition, and also provide a scorecard on how their product / service offering is being measured to achieve the objectives of this condition.
- 1.19 The SAWS respects your privacy and acknowledge that your submission/s will contain personal details, which may belong to you, others and / or to your company (Personal Information). By sending us your submissions, you expressly give us consent to process and further process the Personal Information contained therein which processing will be done in accordance with POPIA, the SAWS POPIA policy and our standard section 18 informed consent documentation which sets out why we need the Personal Information, what we will do with it, and who we will share it with, which you are to familiarise yourself with by downloading it from our website i.e. www.weathersa.co.za
- 1.20 Unless stated otherwise in this Bid or as mutually agreed upon by both parties prior to award of the Bid, all payments due to creditors for goods delivered / services rendered will be settled within thirty (30) days from receipt of an invoice.
- 1.21 In case of a Joint Venture, Consortium, Trust, or Partnership, a signed teaming agreement must be submitted.

2. TAX COMPLIANCE REQUIREMENTS

- 2.1 Bidders must ensure compliance with their tax obligations.
- 2.2 Bidders are required to submit their unique Personal Identification Number (PIN) issued by the South African Revenue Service (SARS) to enable the South African Weather Service to verify the taxpayer’s (Bidder’s) profile and tax status.
- 2.3 Application for a Tax Compliance Status (TCS) Pin may be made via e-filing through the SARS website www.sars.gov.za
- 2.4 Bidders may also submit a printed Tax Compliance Status (TCS) certificate together with the bid.
- 2.5 In bids where consortia / joint ventures / sub-contractors are involved **each** party must submit a separate TCS certificate / Pin / CSD number.
- 2.6 Where no TCS Pin is available but the bidder is registered on the Central Supplier Database (CSD), a

- CSD number must be provided.
- 2.7 No bids will be considered from persons in the service of the state, companies with directors who are persons in the service of the state, or close corporations with members persons in the service of the state.
 - 2.8 Foreign suppliers with neither South African tax obligations nor history of doing business in South Africa must complete the questionnaire on page 2 and 3 of Annexure A. In instances where a recommendation for award of a bid will be made to a foreign bidder, the South African Weather Service will submit the bidders completed Annexure A bid document to the South African Revenue Service. The South African Revenue Service will then issue a confirmation of tax obligations letter to the South African Weather Service confirming whether or not the foreign entity has tax obligations in South Africa.

NB: FAILURE TO PROVIDE / OR COMPLY WITH ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

**PART C
DECLARATION BY BIDDER**

I, in my capacity as hereby declare that I have read and understood the contents and conditions of this bid and certify that the information furnished is true and correct. I accept that, in addition to cancellation of a contract, action may be taken against me should the information provided prove to be false.

Signature:
Date:

Annexure B

General Conditions of Contract

THE NATIONAL TREASURY

Republic of South Africa



GOVERNMENT PROCUREMENT: GENERAL CONDITIONS OF CONTRACT

July 2010

GOVERNMENT PROCUREMENT

GENERAL CONDITIONS OF CONTRACT July 2010

NOTES

The purpose of this document is to:

- (i) Draw special attention to certain general conditions applicable to government bids, contracts and orders; and
- (ii) To ensure that clients be familiar with regard to the rights and obligations of all parties involved in doing business with government.

In this document words in the singular also mean in the plural and vice versa and words in the masculine also mean in the feminine and neuter.

☒ The General Conditions of Contract will form part of all bid documents and may not be amended.

☒ Special Conditions of Contract (SCC) relevant to a specific bid, should be compiled separately for every bid (if applicable) and will supplement the General Conditions of Contract. Whenever there is a conflict, the provisions in the SCC shall prevail.

TABLE OF CLAUSES

1. Definitions
2. Application
3. General
4. Standards
5. Use of contract documents and information; inspection
6. Patent rights
7. Performance security
8. Inspections, tests and analysis
9. Packing
10. Delivery and documents
11. Insurance
12. Transportation
13. Incidental services
14. Spare parts
15. Warranty
16. Payment
17. Prices
18. Contract amendments
19. Assignment
20. Subcontracts
21. Delays in the supplier's performance
22. Penalties
23. Termination for default
24. Dumping and countervailing duties
25. Force Majeure
26. Termination for insolvency
27. Settlement of disputes
28. Limitation of liability
29. Governing language
30. Applicable law
31. Notices
32. Taxes and duties
33. National Industrial Participation Programme (NIPP)
34. Prohibition of restrictive practices

General Conditions of Contract

1. Definitions

1. The following terms shall be interpreted as indicated:
 - 1.1 “Closing time” means the date and hour specified in the bidding documents for the receipt of bids.
 - 1.2 “Contract” means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
 - 1.3 “Contract price” means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.
 - 1.4 “Corrupt practice” means the offering, giving, receiving, or soliciting of any thing of value to influence the action of a public official in the procurement process or in contract execution.
 - 1.5 "Countervailing duties" are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally.
 - 1.6 “Country of origin” means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.
 - 1.7 “Day” means calendar day.
 - 1.8 “Delivery” means delivery in compliance of the conditions of the contract or order.
 - 1.9 “Delivery ex stock” means immediate delivery directly from stock actually on hand.
 - 1.10 “Delivery into consignees store or to his site” means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.
 - 1.11 "Dumping" occurs when a private enterprise abroad market its goods on own initiative in the RSA at lower prices than that of the country of origin and which have the potential to harm the local industries in the

RSA.

1.12 "Force majeure" means an event beyond the control of the supplier and not involving the supplier's fault or negligence and not foreseeable. Such events may include, but is not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

1.13 "Fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the bidder of the benefits of free and open competition.

1.14 "GCC" means the General Conditions of Contract.

1.15 "Goods" means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.

1.16 "Imported content" means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the supplies covered by the bid will be manufactured.

1.17 "Local content" means that portion of the bidding price which is not included in the imported content provided that local manufacture does take place.

1.18 "Manufacture" means the production of products in a factory using labour, materials, components and machinery and includes other related value-adding activities.

1.19 "Order" means an official written order issued for the supply of goods or works or the rendering of a service.

1.20 "Project site," where applicable, means the place indicated in bidding documents.

1.21 "Purchaser" means the organization purchasing the goods.

1.22 "Republic" means the Republic of South Africa.

1.23 "SCC" means the Special Conditions of Contract.

1.24 "Services" means those functional services ancillary to the supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance and other such

obligations of the supplier covered under the contract.

1.25 “Written” or “in writing” means handwritten in ink or any form of electronic or mechanical writing.

2. Application

2.1 These general conditions are applicable to all bids, contracts and orders including bids for functional and professional services, sales, hiring, letting and the granting or acquiring of rights, but excluding immovable property, unless otherwise indicated in the bidding documents.

2.2 Where applicable, special conditions of contract are also laid down to cover specific supplies, services or works.

2.3 Where such special conditions of contract are in conflict with these general conditions, the special conditions shall apply.

3. General

3.1 Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid. Where applicable a non-refundable fee for documents may be charged.

3.2 With certain exceptions, invitations to bid are only published in the Government Tender Bulletin. The Government Tender Bulletin may be obtained directly from the Government Printer, Private Bag X85, Pretoria 0001, or accessed electronically from www.treasury.gov.za

4. Standards

4.1 The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.

5. Use of contract documents and information; inspection.

5.1 The supplier shall not, without the purchaser’s prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

5.2 The supplier shall not, without the purchaser’s prior written consent, make use of any document or information mentioned in GCC clause 5.1 except for purposes of performing the contract.

5.3 Any document, other than the contract itself mentioned in GCC clause 5.1 shall remain the property of the purchaser and shall be returned (all copies) to the purchaser on completion of the supplier’s performance under the contract if so required by the purchaser.

5.4 The supplier shall permit the purchaser to inspect the supplier’s records relating to the performance of the supplier and to have them audited by auditors appointed by the purchaser, if so required by the purchaser.

6. Patent rights

6.1 The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the goods or any part thereof by the purchaser.

7. Performance security

- 7.1 Within thirty (30) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in SCC.
- 7.2 The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.
- 7.3 The performance security shall be denominated in the currency of the contract, or in a freely convertible currency acceptable to the purchaser and shall be in one of the following forms:
- (a) a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in the purchaser's country or abroad, acceptable to the purchaser, in the form provided in the bidding documents or another form acceptable to the purchaser; or
 - (b) a cashier's or certified cheque
- 7.4 The performance security will be discharged by the purchaser and returned to the supplier not later than thirty (30) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified in SCC.

8. Inspections, tests and analyses

- 8.1 All pre-bidding testing will be for the account of the bidder.
- 8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the Department or an organization acting on behalf of the Department.
- 8.3 If there are no inspection requirements indicated in the bidding documents and no mention is made in the contract, but during the contract period it is decided that inspections shall be carried out, the purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.
- 8.4 If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the supplies to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.
- 8.5 Where the supplies or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such supplies or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.
- 8.6 Supplies and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected.
- 8.7 Any contract supplies may on or after delivery be inspected, tested or

analyzed and may be rejected if found not to comply with the requirements of the contract. Such rejected supplies shall be held at the cost and risk of the supplier who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with supplies which do comply with the requirements of the contract. Failing such removal the rejected supplies shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute supplies forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected supplies, purchase such supplies as may be necessary at the expense of the supplier.

8.8 The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 23 of GCC.

9. Packing

9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract, including additional requirements, if any, specified in SCC, and in any subsequent instructions ordered by the purchaser.

10. Delivery and documents

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified in SCC.

10.2 Documents to be submitted by the supplier are specified in SCC.

11. Insurance

11.1 The goods supplied under the contract shall be fully insured in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery in the manner specified in the SCC.

12. Transportation

12.1 Should a price other than an all-inclusive delivered price be required, this shall be specified in the SCC.

13. Incidental services

13.1 The supplier may be required to provide any or all of the following services, including additional services, if any, specified in SCC:

- (a) performance or supervision of on-site assembly and/or commissioning of the supplied goods;
- (b) furnishing of tools required for assembly and/or maintenance of the supplied goods;
- (c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;

- (d) performance or supervision or maintenance and/or repair of the supplied goods, for a period of time agreed by the parties, provided that this service shall not relieve the supplier of any warranty obligations under this contract; and
- (e) training of the purchaser's personnel, at the supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied goods.

13.2 Prices charged by the supplier for incidental services, if not included in the contract price for the goods, shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the supplier for similar services.

14. Spare parts

14.1 As specified in SCC, the supplier may be required to provide any or all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier:

- (a) such spare parts as the purchaser may elect to purchase from the supplier, provided that this election shall not relieve the supplier of any warranty obligations under the contract; and
- (b) in the event of termination of production of the spare parts:
 - (i) Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and
 - (ii) following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15. Warranty

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications) or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.2 This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in SCC.

15.3 The purchaser shall promptly notify the supplier in writing of any claims arising under this warranty.

15.4 Upon receipt of such notice, the supplier shall, within the period specified in SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.5 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in SCC, the purchaser may proceed to take

such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16. Payment
- 16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in SCC.
- 16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfillment of other obligations stipulated in the contract.
- 16.3 Payments shall be made promptly by the purchaser, but in no case later than thirty (30) days after submission of an invoice or claim by the supplier.
- 16.4 Payment will be made in Rand unless otherwise stipulated in SCC.
17. Prices
- 17.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in his bid, with the exception of any price adjustments authorized in SCC or in the purchaser's request for bid validity extension, as the case may be.
18. Contract amendments
- 18.1 No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties concerned.
19. Assignment
- 19.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the purchaser's prior written consent.
20. Subcontracts
- 20.1 The supplier shall notify the purchaser in writing of all subcontracts awarded under this contracts if not already specified in the bid. Such notification, in the original bid or later, shall not relieve the supplier from any liability or obligation under the contract.
21. Delays in the supplier's performance
- 21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.
- 21.2 If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.
- 21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.
- 21.4 The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the

supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.

21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 21.2 without the application of penalties.

21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without canceling the contract, be entitled to purchase supplies of a similar quality and up to the same quantity in substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and without prejudice to his other rights, be entitled to claim damages from the supplier.

22. Penalties

22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services using the current prime interest rate calculated for each day of the delay until actual delivery or performance. The purchaser may also consider termination of the contract pursuant to GCC Clause 23.

23. Termination for default

23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:

- (a) if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;
- (b) if the Supplier fails to perform any other obligation(s) under the contract; or
- (c) if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

23.2 In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.

23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.

23.4 If a purchaser intends imposing a restriction on a supplier or any

person associated with the supplier, the supplier will be allowed a time period of not more than fourteen (14) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated fourteen (14) days the purchaser may regard the intended penalty as not objected against and may impose it on the supplier.

23.5 Any restriction imposed on any person by the Accounting Officer / Authority will, at the discretion of the Accounting Officer / Authority, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person, is or was in the opinion of the Accounting Officer / Authority actively associated.

23.6 If a restriction is imposed, the purchaser must, within five (5) working days of such imposition, furnish the National Treasury, with the following information:

- (i) the name and address of the supplier and / or person restricted by the purchaser;
- (ii) the date of commencement of the restriction
- (iii) the period of restriction; and
- (iv) the reasons for the restriction.

These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.7 If a court of law convicts a person of an offence as contemplated in sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.

24. Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or anti-dumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidized import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall on demand be paid forthwith by the contractor to the State or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which

may be due to him

25. Force Majeure

25.1 Notwithstanding the provisions of GCC Clauses 22 and 23, the supplier shall not be liable for forfeiture of its performance security, damages, or termination for default if and to the extent that his delay in performance or other failure to perform his obligations under the contract is the result of an event of force majeure.

25.2 If a force majeure situation arises, the supplier shall promptly notify the purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

26. Termination for insolvency

26.1 The purchaser may at any time terminate the contract by giving written notice to the supplier if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

27. Settlement of Disputes

27.1 If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

27.2 If, after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

27.3 Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.

27.4 Mediation proceedings shall be conducted in accordance with the rules of procedure specified in the SCC.

27.5 Notwithstanding any reference to mediation and/or court proceedings herein,

- (a) the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and
- (b) the purchaser shall pay the supplier any monies due the supplier.

28. Limitation of liability

28.1 Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Clause 6;
(a) the supplier shall not be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser; and

	(b) the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the total contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.
29. Governing language	29.1 The contract shall be written in English. All correspondence and other documents pertaining to the contract that is exchanged by the parties shall also be written in English.
30. Applicable law	30.1 The contract shall be interpreted in accordance with South African laws, unless otherwise specified in SCC.
31. Notices	31.1 Every written acceptance of a bid shall be posted to the supplier concerned by registered or certified mail and any other notice to him shall be posted by ordinary mail to the address furnished in his bid or to the address notified later by him in writing and such posting shall be deemed to be proper service of such notice 31.2 The time mentioned in the contract documents for performing any act after such aforesaid notice has been given, shall be reckoned from the date of posting of such notice.
32. Taxes and duties	32.1 A foreign supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the purchaser's country. 32.2 A local supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted goods to the purchaser. 32.3 No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid the Department must be in possession of a tax clearance certificate, submitted by the bidder. This certificate must be an original issued by the South African Revenue Services.
33. National Industrial Participation (NIP) Programme	33.1 The NIP Programme administered by the Department of Trade and Industry shall be applicable to all contracts that are subject to the NIP obligation.
34 Prohibition of Restrictive practices	34.1 In terms of section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, an agreement between, or concerted practice by, firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder (s) is / are or a contractor(s) was / were involved in collusive bidding (or bid rigging). 34.2 If a bidder(s) or contractor(s), based on reasonable grounds or evidence obtained by the purchaser, has / have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in the Competition Act No. 89 of 1998.

- 34.3 If a bidder(s) or contractor(s), has / have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and / or terminate the contract in whole or part, and / or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding ten (10) years and / or claim damages from the bidder(s) or contractor(s) concerned.

Annexure C

Bidder's Disclosure

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. Bidder's declaration

2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest¹ in the enterprise, employed by the state? **YES/NO**

2.1.1 If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below.

Full Name	Identity Number	Name of State institution

¹ the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise.

2.2 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution? **YES/NO**

2.2.1 If so, furnish particulars:

.....
.....

2.3 Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract? **YES/NO**

2.3.1 If so, furnish particulars:

.....
.....

3 DECLARATION

I, the undersigned, (name).....

..... in submitting the accompanying bid, do hereby make the following statements that I certify to be true and complete in every respect:

- 3.1 I have read and I understand the contents of this disclosure;
- 3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;
- 3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium² will not be construed as collusive bidding.
- 3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.
- 3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.
- 3.5 There have been no consultations, communications, agreements or

² Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

arrangements made by the bidder with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.

- 3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT.

I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

.....
Signature

.....
Date

.....
Position

.....
Name of bidder

Annexure F

Preference Points Claim Form in terms of the
Preferential Procurement Regulations 2022

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to tender:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 To be completed by the organ of state

The applicable preference point system for this tender is the **80/20** preference point system.

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:

- (a) Price; and
- (b) Specific Goals.

1.4 To be completed by the organ of state:

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	80
SPECIFIC GOALS	20
Total points for Price and SPECIFIC GOALS	100

1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.

- 1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

- (a) “**tender**” means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;
- (b) “**price**” means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;
- (c) “**rand value**” means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;
- (d) “**tender for income-generating contracts**” means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and
- (e) “**the Act**” means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \mathbf{Ps} = \mathbf{80} \left(\mathbf{1} - \frac{\mathbf{Pt} - \mathbf{Pmin}}{\mathbf{Pmin}} \right) & \mathbf{or} & \mathbf{Ps} = \mathbf{90} \left(\mathbf{1} - \frac{\mathbf{Pt} - \mathbf{Pmin}}{\mathbf{Pmin}} \right) \end{array}$$

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

3.2. FORMULAE FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT

3.2.1. POINTS AWARDED FOR PRICE

A maximum of 80 or 90 points is allocated for price on the following basis:

$$Ps = 80 \left(1 + \frac{Pt - Pmax}{Pmax} \right) \text{ or } Ps = 90 \left(1 + \frac{Pt - Pmax}{Pmax} \right)$$

Where

- Ps = Points scored for price of tender under consideration
Pt = Price of tender under consideration
Pmax = Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

- 4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:
- 4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—
- (a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or
 - (b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,
- then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.

(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.

Note to tenderers: The tenderer must indicate how they claim points for each preference point system.)

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer)
B-BBEE Status Level of Contributor		
Level 1	20	
Level 2	18	
Level 3	14	
Level 4	12	
Level 5	8	
Level 6	6	
Level 7	4	
Level 8	2	
Non-compliant contributor	0	

DECLARATION WITH REGARD TO COMPANY/FIRM

4.3. Name of company/firm.....

4.4. Company registration number:

4.5. TYPE OF COMPANY/ FIRM

- Partnership/Joint Venture / Consortium
- One-person business/sole propriety
- Close corporation
- Public Company
- Personal Liability Company
- (Pty) Limited
- Non-Profit Company
- State Owned Company

[TICK APPLICABLE BOX]

4.6. I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:

- i) The information furnished is true and correct;
- ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
- iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;
- iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –
 - (a) disqualify the person from the tendering process;
 - (b) recover costs, losses or damages it has incurred or suffered as a result of that person’s conduct;
 - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
 - (d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
 - (e) forward the matter for criminal prosecution, if deemed necessary.

.....	
SIGNATURE(S) OF TENDERER(S)	
SURNAME AND NAME:
DATE:
ADDRESS:

Annexure G

Pricing Schedule for Services

1.1.3 Cost break-down of ceiling price in 1.1.1

Bidders are required to indicate the cost component/s used for determining the ceiling price as given in 1.1.1 above.

Description	Cost (VAT Incl.)

1.1.4 Period required for commencement of the project after acceptance of bid?

1.1.5 Are the rates quoted firm for the full period of the project?

YES	*NO
-----	-----

1.1.6 *If not firm for the full period, provide details of the basis on which adjustments will be applied for, for example consumer price index.

Annexure H

Specifications / Terms of Reference for bids

1 DESCRIPTION

The South African Weather Service (SAWS) seek for the service provider to provide the eSignature annual subscription license for a period of 3 years. The solution must be cloud-based.

2 INTRODUCTION

The South African Weather Service (SAWS) is a public entity of the Department of Forestry, Fisheries and the Environment (DFFE) and derives its mandate from the South African Weather Service Act (No 8 of 2001 as amended). The public entity is listed as a Schedule 3A Public Entity in terms of the Public Finance Management Act (PFMA).

SAWS is tasked with providing timely and accurate scientific data in the field of meteorology to the broader South African society: a combination of both public good and commercial services. The organisation plays a vital role in South African public life, not just as a provider of key services, but also in empowering citizens to adapt the effects of the ever-changing weather.

3 BACKGROUND

South African Weather Service (SAWS) currently has an eSignature solution for accommodating 7000 envelopes and unlimited users. The current contract is due to expire, hence the necessity to procure a new eSignature solution.

4 REQUIREMENT / SCOPE OF WORK

4.1 Technical / Functional requirements

This bid calls for the appointment of a service provider or Reseller Partner to supply eSignature solutions to sign official documents.

SAWS ICT is requesting to source eSignature annual subscription license for business continuity. SAWS has been using eSignature solution for the past five years.

It is required that a Service Provider be appointed to supply and implement an e-Signature solution to enable the reviewing, tracking and signing of electronic documents. The solution will aid business continuity and efficiency as approvals can be made using this e-Signature Solution

This subscription model is the preferred option to ensure that the envelope usage by users does not exceed the target limit. The current package is based on envelope subscription not the seat subscription. The period of service will be for three years.

BUSINESS REQUIREMENTS	
1	<p>Solution Accessibility</p> <p>a) The electronic solution should be provided as cloud based.</p> <p>b) The solution should be accessible from anywhere on any device and allow you to view and sign documents on the go:</p> <ul style="list-style-type: none"> • Accessible through all web browsers, desktop, and mobile applications. • Offers compatibility to view and sign documents from mobile devices, such as phones and tablets, via mobile app or mobile web browser. • Accessible through a secure (TLS/SSL-enabled) web service.
2	<p>Logging in to The Solution</p> <p>a) Allow single sign-on (SSO) to permit one set of login credentials to access multiple applications and to ensure compliance with the organization’s security and policies.</p>
3	<p>Electronic Signature Options</p> <p>a) Ability to customize electronic signature.</p> <p>b) The solution should offer different signature options such as typed, drawn or uploaded signatures as images.</p>
4	<p>Document Creation</p> <p>a) Ability to personally sign or request signatures.</p> <p>b) Ability to upload documents from the most widely used cloud storage services, such as Microsoft Office 365, Microsoft OneDrive, Google Drive etc.</p> <p>c) Ability to support multi-document type support such as .doc, .docx, .pdf, .pptx, .xls, xlsx, .txt etc. and automatically convert final document to pdf format.</p> <p>d) Ability to upload and attach supporting documents as part of the signing process or sign acknowledgment.</p> <p>e) Ability to sign scrollable pdf files and allow scrolls even after signing.</p> <p>f) Ability to add data fields such as checkboxes, radio buttons, dropdown tags, text, date etc. to the documents to be signed and automatically converted to PDF for signature</p> <p>g) Ability to create a standard template with defined recipient roles and signing and information fields.</p> <p>h) Ability to copy people who are not part of the signing process to receive fully signed documents after all signatories have signed.</p> <p>i) Ability to correct or make changes to a document in a signing process by the initiator instead of aborting the process</p>
	<p>Sending Options</p> <p>a) One send/transaction should include any number of recipients and any number of documents.</p>

5	<ul style="list-style-type: none"> b) Automatic signer fields placement. c) Ability to route documents to multiple users in serial, parallel and mixed sequencing.
6	<p>Signing Process</p> <ul style="list-style-type: none"> a) Ability to zoom in/out on the documents on the system sent for signatures for better viewing. b) Ability to automatically guide signers where to sign. c) Ability to delegate the document to a different user. d) Ability to enable a user to be granted permission to send or manage documents. e) The solution should convert the final document to PDF format. f) Ability to decline the document in a signing process by the recipient.
7	<p>Collaboration</p> <ul style="list-style-type: none"> a) Multiple users to collaborate on a document, including adding comments and making edits before it is signed. b) Ability to ask and answer questions about documents and receive real-time comment notifications.
8	<p>Provide Audit Trails</p> <ul style="list-style-type: none"> a) Real-time audit trail reporting and tracking of documents, ability to see detailed status for each recipient and individual report portal including viewing, printing, sending, signing, or declining to sign a document. b) An audit trail of the document workflow information should be retained for proof of compliance, from initiation to completion. Audit trail must be kept for a minimum period of 6 months. c) It should provide the ability for real-time visibility of the status the document sign-off request is in. This will enable the user requesting sign-off to know when the document is opened; signed; or returned.
9	<p>Security and Privacy</p> <ul style="list-style-type: none"> a) Meets global security standards and use of the strongest data encryption technologies available, such as Advanced Encryption Standard (AES) 128-bit encryption and Secure Sockets Layer (SSL) 256-bit encryption to ensure documents in the system are encrypted.
10	<p>Compliance</p> <ul style="list-style-type: none"> a) Comply with the applicable guidelines or requirements specified in DPSA Electronic Signature Guidelines Appendices version 1.1.0 (Attached as Annexure H1). b) Every signed document should come with a certificate of completion that provides proof of the signing process to all parties of the transaction. c) This certificate should include information from the audit trail, proving who signed, timestamps detailing when and where each person signed, and the completed document itself. d) Legal Notice ensures that contracts and signatures cannot be denied validity or enforceability because they are in electronic form.

	<p>e) Disclosure, to be compliant with organization policy, requiring signers to consent to the Electronic Record and Signature Disclosure notice.</p> <p>f) Ability to specify a custom watermark to differentiate draft documents from completed signed documents.</p>
11	<p>Hosting</p> <p>a) The solution must be hosted within the boundaries of South Africa.</p>
12	<p>Solution Availability</p> <p>a) The solution should deliver 99.99% uptime with no maintenance downtime during normal business hours.</p> <p>b) The eSignature should be available 24/7 and should allow users to sign within the SAWS network even via VPN.</p>
13	<p>Reporting</p> <p>a) To generate monthly report of subscription summary, number of active/pending users including administrators and envelopes (pro rate envelope sends, envelope sent, envelope trending),</p> <p>b) To generate monthly reports of volume trend for envelopes (completed/Sent/Declined/ and Voided),</p> <p>c) To generate envelope velocity by showing completion time of envelopes, total envelopes percentage and total files etc., and</p> <p>d) To show each user’s activity and success rate</p>

4.2 Training And Skills Transfer:

- Training of SAWS officials
 - 5 ICT Resources (Once-off training/ skills transfer)
 - 67 Users
- On the usability of the system during the project implementation/onboarding process.
- The bidder to factor in the possibility of refresher training and training of new officials (new starts in the organization) after project sign-off.
- The bidder to be able to conduct the training withing two (2) weeks.
- Provision of technical and user manuals.

4.3 Project Management/Consulting Services

Involve the planning, execution, and oversight of projects to ensure successful delivery within scope, time, and budget. These services must include project planning, resource coordination, risk management, progress monitoring, and quality assurance. In addition, consulting support must offer expert guidance, process improvement, strategic alignment, and capacity building to help organizations enhance their project delivery capabilities.

4.4 Support

Template: Specifications / Terms of Reference for bids – Annexure H



The service provider will be expected to provide technical support via email or through the phone for a period of three years. The support will also include upgrades, patches and updates of the eSignature system. For the purpose of this bid business hours are defined as Monday to Friday from 08:00am to 05:30pm, excluding public holidays.

The supplier Help desk shall be available during business hours for software support.

Priority	Description	Response time
Priority 1 – Critical	Critical service is unavailable or seriously impaired due to a problem. The impact on normal business operations is severe. Adverse business impact.	4 - hour response time
Priority 2 – High	Disruption of a service and/or operations. Ramifications include some impact on the business and operations.	6 - hour response time
Priority 3 – Medium	A non-critical service is impacted. There is a minor impact on normal business operations.	8 - hour response time
Priority 4 - Low	A non-critical service is impacted. There is no direct impact on the normal business operations	24 -hour response time

5 EVALUATION PROCESS

The bid will be evaluated in 4 phases as mentioned below:

- **Phase 1: SCM Administrative Requirements.**
- **Phase 2: Mandatory Requirements.**
- **Phase 3: Functional Evaluation.**
- **Phase 4: Price and Specific Goals.**

5.1 Phase 1: SCM Administrative Requirements

Bids received will be verified for completeness and correctness. SAWS reserves the right to accept or reject a bid based on the completeness and correctness of the documentation and information provided.

Bidders are to ensure that they submit the following documentation / information with their bid.

Document	Comments
Proof of registration on the Central Supplier Database (CSD) of National Treasury	Bidders must be registered on the CSD. CSD registration number must be provided.



Bid Invitation (Annexure A)	Completed and signed
SBD 3.3 for services (Pricing Schedule)	Completed
SBD 4 (Bidder’s Declaration)	Completed and signed
SBD 6.1 (Preference Points Claim Form)	Completed and signed if points are claimed
SARS (South African Revenue Service) Tax Compliant	Bidders tax matters must be in order
BBBEE Certificate	Valid and compliant original B-BBEE and/or certified copies of Sworn Affidavit must be submitted for any points claimed

5.2 Phase 2: Mandatory Technical / Functional requirements

The following mandatory requirements must be complied with by the bidder.

5.2.1 Section 1: Attendance of Compulsory Briefing Session and OEM Accreditation and Support

Please note that bidders will not be evaluated further (Section 2: Solution Compliance) if they do not provide evidence confirming compliance with the specified mandatory requirement in the table below.

	Mandatory Technical / Functional requirements	Evidence to be submitted with bid
1	Attendance of compulsory briefing session by bidder.	Bidders must ensure that they attend the compulsory briefing session.
2	Bidder must be appropriately accredited to supply, implement, and support the required solution (Attach Proof of OEM accreditation) or authorized reseller letter.	Bidder to provide a valid Certificate or letter of OEM accreditation. (SAWS reserve the right to verify the validity of the Certificate or Letter)

Bidders who comply with the mandatory requirements will be considered for further evaluation.

5.2.2 Section 2: Solution Compliance

Template: Specifications / Terms of Reference for bids – Annexure H



Please note that bidders will not be evaluated further (Section 3: Support) if they do not confirm compliance with the specified mandatory requirement in the table below.

Detailed proposal of the suggested Electronic Signature Solution on the company letterhead as per the 13 items specified in the scope. No generic OEM product brochures will be considered.

Bidders must indicate in the table below if their offer comply or do not comply with each of the requirements by indicating “Yes” or “No” next to each requirement. **Failure by a bidder to indicate “Yes” or “No” in the table below next to each of the requirements will lead to the bidder being disqualified.**

No.	Functions & Features	Comply (Yes / No)	Document reference / Page no.
1.	Solution Accessibility		
2.	Logging in to The Solution		
3.	Electronic Signature Options		
4.	Document Creation		
5.	Sending Options		
6.	Signing Process		
7.	Collaboration		
8.	Provide Audit Trails		
9.	Security and Privacy		
10.	Compliance		
11.	Hosting		
12.	Solution Availability		
13.	Reporting		

5.2.3 Section 3: Support

Please note that bidders will not be evaluated further (Phase 3: Functional Evaluation) if they do not confirm compliance with the specified mandatory requirement in the table below

The service provider will be expected to provide technical support via email or through the phone for a period of three years. The support will also include upgrades, patches and updates of the eSignature system. For the purpose of this bid business hours are defined as Monday to Friday from 08:00am to 05:30pm, excluding public holidays. Bidders must indicate in the table below if their offer comply or do not comply with each of the requirements by indicating “Yes” or “No” next to each requirement. **Failure by a bidder to indicate “Yes” or “No” in the table below next to each of the requirements will lead to the bidder being disqualified**

Priority	Description	Response time	Comply (Yes / No)
Priority 1 – Critical	Critical service is unavailable or seriously impaired due to a problem. The impact on normal business operations is severe. Adverse business impact.	4 -hour response time	
Priority 2 – High	Disruption of a service and/or operations. Ramifications include some impact on the business and operations.	6 - hour response time	
Priority 3 – Medium	A non-critical service is impacted. There is a minor impact on normal business operations.	8 - hour response time	
Priority 4 - Low	A non-critical service is impacted. There is no direct impact on the normal business operations	24 -hour response time	

5.3 Phase 3: Functional evaluation

Technical / Functional evaluation of the bid will be done in terms of the criteria as stated in the table below. Bidders should take note of the Criterion, Weighting & Scoring when responding to this bid.

Criterion	Weight	Score
-----------	--------	-------

Template: Specifications / Terms of Reference for bids – Annexure H



<p>1</p>	<p>Contactable References Bidder to provide reference letters (dated not older than 5 years) for electronic or digital signature deployments provided to clients.</p> <p>Each reference letter provided must:</p> <ul style="list-style-type: none"> • Be on client’s company letter head. • Be signed by the client. • Be dated. • Include the contact details of the client. (e.g. Physical Address, e-mail, Telephone, etc.). • Include a brief description of the electronic or digital signature solution provided to the client by the bidder. (The solution must be specific to the solution offered to SAWS.) <p>SAWS reserve the right to contact due diligence on references provided.</p>	<p>50</p>	<p>50 = Five or more reference letters provided. 40 = Three or Four reference letters provided. 30 = Two reference letters provided. 10 = One reference letter provided. 0 = No reference letters provided or reference letter/s not meeting all the requirements.</p>
<p>2</p>	<p>Approach and Methodology</p> <p>The bidder must provide a Project Plan with timelines. The Project plan must include the following:</p> <ul style="list-style-type: none"> • Project Plan activities clearly defined. • Project Resources. • On-boarding of users. • Training Plan / Programme. • Timeline (number of weeks) from award of bid to go-live. 	<p>50</p>	<p>50 = Project Plan provided meeting all the requirements with a timeline of 2 weeks or less. 40 = Project Plan provided meeting all the requirements with a timeline of more than 2 weeks up to 4 weeks. 30 = Project Plan provided meeting all the requirements with a timeline of more than 4 weeks up to 6 weeks. 10 = Project Plan provided meeting all the requirements with a timeline of more than 6 weeks. 0 = Project Plan not provided or Project Plan provided not meeting all the requirements.</p>
<p>TOTAL</p>		<p>100</p>	

Bidders who score 70% and more will qualify for further evaluation in terms of Price and Specific Goals.

5.4 Phase 4: Price and Specific Goals evaluation

Bidders who comply with the requirements of this bid will be evaluated according to the preference point scoring system as determined in the Preferential Procurement Regulations, 2022 pertaining to the Preferential Procurement Policy Framework Act, Act No 5 of 2000.

The following preference point systems are applicable to all bids:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

The value of this bid is estimated NOT to exceed R50 000 000 (all applicable taxes included) and therefore the 80/20 preference point system shall be applicable.

Points for this bid shall be awarded for:

- (a) Price; and
- (b) Specific Goals (Refer to Annexure F: Preference Points Claim Form).

The maximum points for this bid are allocated as follows:

	POINTS
PRICE	80
SPECIFIC GOALS (Refer to Annexure F: Preference Points Claim Form)	20
Total points for Price and Specific Goals	100

Subject to section 2(1)(f) of the Preferential Procurement Policy Framework Act, 2000 (Act no 5 of 2000), the tender will be awarded to the tenderer scoring the highest points.

6. DUE DILIGENCE

The South African Weather Service reserves the right to conduct supplier due diligence prior to final award or at any time during the contract period. This may include site visits, reference checks and requests for additional information.

7. SPECIAL CONDITIONS OF CONTRACT

This bid and all contract emanating there from will be subject to the General Conditions of Contract (GCC) issued in accordance with Chapter 16A of the Treasury Regulations published in terms of the Public Finance

Management Act, 1999 (Act 1 of 1999). The Special Conditions are supplement to that of the General Conditions of Contract. Where, however the Special Conditions of Contract are in conflict with the General Conditions of Contract, the Special Conditions of the Contract prevail.

- 7.1 Physical Address:
South African Weather Service
1263 Heuwel Road
Centurion
0157

ANNEXURE H1



ELECTRONIC SIGNATURE GUIDELINES

Version 1.1.0

February 12, 2019

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

Document Version Control

Date	Author	Version
12 February 2019	DPSA	Version 1.1.0

Approvals

The Electronic Signature Guidelines are approved by the Minister for Public Service and Administration.

Name	Signature	Date

Review Period

This guidelines will be reviewed annually or subsequent to any significant issue arising that has not been considered

Name	Signature	Date

Contact Information

For more information on this policy or to inquire about a variation that is not covered, email at:

Morena.Monareng@dpsa.gov.za

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

TABLE OF CONTENTS

1. INTRODUCTION.....	4
2. PURPOSE	4
3. SCOPE.....	4
4. LEGAL USE OF ELECTRONIC SIGNATURES IN SOUTH AFRICA.....	5
5. GUIDELINES FOR ELECTRONIC RECORDS	9
6. RISK MANAGEMENT OF ELECTRONIC RECORDS	12
7. ELECTRONIC SIGNATURE GOVERNANCE.....	14
8. PLANNING OVERVIEW FOR AN ELECTRONIC SIGNATURE PROGRAMME	15
9. STEPS FOR AN ELECTRONIC SIGNATURES PROGRAMME.....	18
10. REFERENCES	23
11. APPENDICES	23

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

Definitions/Glossary

DPSA	Department of Public Service and Administration
GCIO	Government Chief Information Office
GITOC	Government Information Technology Officer Council
SITA	State Information Technology Agency
PSA	Public Service Act
PFMA	Public Finance Management Act
POPI	The Protection of Personal Information Act
PAIA	Promotion of Access to Information Act
ICT	Information and Communications Technology
SSA	State Security Agency
MISS	Minimum Information Security Standards
ISO	International Standards Organisation
ISACA	Information Systems Audit and Control Association
NIST	The National Institute of Standards and Technology
SCISS	Standing Committee on Information Systems
ECT	Electronic Communication and Transactions Act, 2002
SAAA	South African Accreditation Authority
PKI	Public Key Infrastructure
AES	Advanced Electronic Signature
SACA	The South Africa Certification Authority
CA	Certification Authority
RA	Registration Authority
CPS	Certification Practice Statement
SAPO	South Africa Post Office

Relevant legislation

Public Service Act, 1994
Public Service Regulations, 2016
Promotion of Access to Information Act, 2000
The Protection of Personal Information Act, 2013
State Information Technology Agency Act, 1998
Intelligence Services Act, 2002
National Archives of South Africa Act, 1996
Electronic Communication and Transactions Act, 2002

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

1. INTRODUCTION

- 1.1** The development of electronic government (e-government) and electronic services (e-services) is changing the way public service departments deliver services. As a result, electronic systems and processes are becoming as important as a written signature on paper. In a paper environment, a hand signature authorises and authenticates the content of a document. A signature provides a level of trustworthiness and accountability that aids the conduct of business. Electronic signatures extend the function of handwritten signatures to electronic documents, providing a way for two parties to conduct business confidently in an electronic environment.
- 1.2** In an effort to support the implementation of an electronic signature solution within the public service, the DPSA developed these generic Electronic Signature Guidelines (hereafter referred to as the “Guidelines”). The Guidelines were developed in collaboration with key ICT security stakeholders in government, such as the GITOC and the SCISS.
- 1.3** These Guidelines are meant to be referenced by departments planning to utilise electronic signatures and their intent is to:
- provide the framework for evaluating the appropriateness of an electronic signature technology for an intended purpose;
 - enable greater adoption of digital signature technology across government to streamline business processes, and increase information security.
- 1.4** The ECT Act established the legal definition for the use of electronic signatures. In terms of the ECT Act, an electronic signature is defined as “*data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature*”. To determine the risks and security associated with the use of electronic signatures, departments should undertake a risk-based evaluation using the National Treasury Public Sector Risk Management Framework 2010.
- 1.5** For the purpose of these Guidelines, reference to a “department/s” means a national department, a provincial department and a national or provincial government component as per the Public Service Act, 1994.

2. PURPOSE

- 2.1** The Guidelines are to provide guidance for departments on planning and deploying electronic signatures or digital signatures or advanced electronic solutions to modernise the department’s internal efficiency and ensure delivery of the department’s constitutional service delivery mandate and objectives.

3. SCOPE

- 3.1** The Guidelines covers considerations for using electronic signatures as an authentication mechanism of government documents.

3.2 Where relevant laws are referenced, these guidelines are not a substitute for professional guidance on legal matters.

3.3 These guidelines are primarily intended for use by:

- a) GITO's of departments;
- b) Information Technology Security Officers;
- c) GITOC;
- d) Government Chief Information Office.

To support the digitisation of services and internal processes, departments are encouraged to consider deploying electronic signature programmes.

4. LEGAL USE OF ELECTRONIC SIGNATURES IN SOUTH AFRICA

4.1 Electronic Signatures in South Africa

4.1.1 The use of electronic signatures in government is recognised under the ECT Act. The ECT Act provides assurance that electronic signatures will be granted the same legal authority as written signatures on paper. Therefore, if an electronic transaction meets the requirements of the electronic signature laws, neither party can repudiate a transaction based on the fact that the transaction was conducted electronically, rather than on paper. Further details on the ECT Act and electronic signatures are discussed in Appendix A.

4.1.2 Electronic signatures (Figure 1 below) come in various forms and have the capacity to meet various purposes (authentication, approval, integrity) and various uses (evidentiary, recordkeeping, etc.). In most cases, a signature required under legislation can be met using a digital alternative and will be deemed equivalent to a written signature provided it meets the criteria stipulated in the ECT Act.

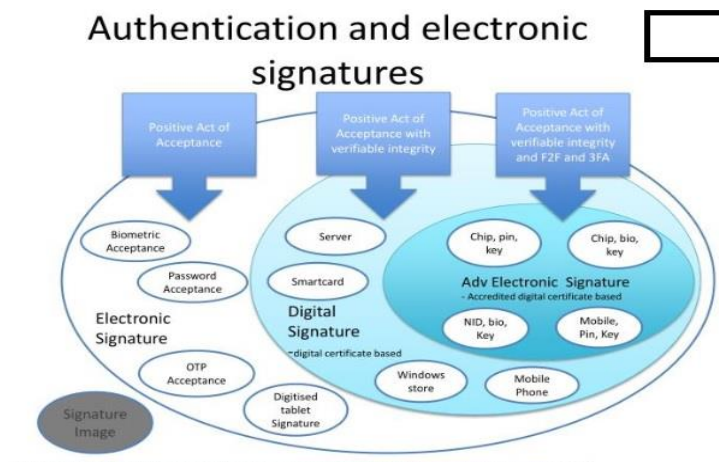


Figure 1 Electronic Signature Types as defined in the ECT Act. (Adapted from Lawtrust Ltd)

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

- 4.1.3** For many day-to-day operations, a simple electronic signature (generated through authentication or “click to accept” process) is adequate to indicate that an individual has demonstrated intent to sign or approve a transaction. Other cases will require or prefer the use of a digital signature or advanced electronic signature.
- 4.1.4** A digital signature is a very specific form of an electronic signature that uses cryptography to establish the authenticity and validity of the signature with much greater certainty.
- 4.1.5** An advanced electronic signature is a digital signature created with a digital certificate from the South African Accreditation Authority (SAAA) under section 37 of the ECT Act, following a face-to-face identification process with the user. An advanced electronic signature is deemed reliable in law and is accepted as prima facie proof of validity, i.e., is always assured to be valid and have been applied correctly, to eliminate the burden of proof. In terms of section 13 of the ECT Act, where the signature of a person is required by law and such law does not specify the type of signature required, an advanced electronic signature must be used. It must be noted that a written signature is still applicable. It is only when an electronic signature is the preferred option that one would be obliged to use an advanced electronic signature.

4.2 ELECTRONIC SIGNATURE

- 4.2.1** An electronic signature must be a positive act of acceptance – visible, understandable and fair and must identify the signatory and be verifiable.
- 4.2.2** As per section 13 of the ECT Act, where an electronic signature is required, and where parties have not agreed to the type of electronic signature to be used, the signature requirement is met if –
- a) *“ a method used identifies the person and indicates the person’s approval of the information; and*
 - b) *having regard to all relevant circumstances at the time the method was used, the method was reliable and appropriate for the purpose for which the information was communicated.”*

4.3 DIGITAL SIGNATURE

- 4.3.1** A digital signature (although not defined in the ECT Act), is a signature that originates with a digital certificate.
- 4.3.2** A digital certificate is issued to a person, once that person has been verified as the person who they claimed to be.
- 4.3.3** A digital signature requires not only a positive act of acceptance but also has verifiable integrity as a result of a digital certificate.
- 4.3.4** A digital certificate is a positive identification of a device/server or entity that operates very similar to how an identity document identifies a specific person.

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

4.3.5 A digital certificate is managed by a Public Key Infrastructure (PKI), which is a combination of hardware, software, and procedures implemented in order to manage digital certificates.

4.4 ADVANCED ELECTRONIC SIGNATURES (AES)

4.4.1 An AES is defined in the ECT Act as “an electronic signature which results from a process which has been accredited by the Authority¹ as provided for in section 37”.

4.4.2 That is, an AES is a digital certificate based signature, which utilises mechanisms to ensure security and integrity, as well as to confirm the identity of the signatory.

4.4.3 An AES consists of a positive act of acceptance, together with verifiable integrity (digital certificate based on confirmation of the identity of the applicant) with an added face-to-face verification mechanism, as well as 3-factor authentication (or similar). The 3-factor authentication is briefly:

- a. Something you are (biometrics such as fingerprint and iris scan);
- b. Something you know (pin, password, passphrase or secret question);
- c. Something you have (key, device).

What are the three factors



Figure 2 What are the three factors

4.4.4 The 3-factor authentication makes the AES strong, reliant and trustworthy.

4.4.5 Section 13(4) of the ECT Act states that “ where an AES has been used, such signature is regarded as being a valid electronic signature and to have been applied properly unless the contrary is proved.”

4.4.6 An AES is the most secure signature available in South Africa. Even though it does not have to be applied to all documents, the user has the option available to use it on all documents. For documents not demanding an AES and not excluded by the ECT Act, an electronic signature would suffice.

¹ South African Accreditation Authority

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

4.5 PUBLIC KEY INFRASTRUCTURE (PKI)

4.5.1 Electronic signatures based on PKI (digital signatures and AES) use an algorithm in order to generate two keys, private and public, that are mathematically linked to each other.

4.5.2 In order to create a digital signature, software is utilised to create a one-way hash (cryptographic process) of the electronic document that is to be signed. The private key that was generated, is used to encrypt the hash. The encrypted hash, with other information such as the hashing algorithm, constitutes the digital signature.

4.5.3 The hash value is unique and prevents any subsequent changes to the document signed (which will alter the hash value and warn the recipient of alterations to the document). The digital certificate used to create a digital signature on an electronic document links a public key to an identity and can be utilised to confirm who the owner of that public key is.

4.6 DIGITAL SIGNATURE CERTIFICATES

4.6.1 A digital certificate (APPENDIX D) is an electronic file securely linking an individual to encryption keys and identification data. This certificate belongs to a server or person and resides on a mobile token or within the certificate store of an application like an internet browser – encrypting and signing communications and transactions, protecting them from being intercepted by any unauthorised third party.

4.7 TYPES OF DIGITAL SIGNATURE CERTIFICATES

4.7.1 There are three (3) types of digital certificates and are applied depending upon the assurance level and usage requirements.

The following table provides an overview of the different types of digital certificates and the level of assurance.

Type of Certificate	Description and Assurance level
Class 2 certificate	Medium assurance 1024-bit certificates that are for standard commercial use . These certificates are ideal for medium-level authentication, signing, and encryption of electronic communications like email
Class 3 certificate	High assurance , closed community certificates for commercial use. These certificates are only available to organisations who wish to authenticate users within their own closed user groups (staff and/or customers). They are ideal for high-level authentication, access control, signing and encryption of electronic communications, transactions and processes within a closed environment.
Advanced Electronic Signatures (Class 4 Certificates)	Advanced Electronic Signature . These certificates are available to users and organisations that wish to transact and communicate with clear legal status. A high level of independent identity authentication is provided through the collection of personal identity information, including fingerprints, and the verification of the information provided by the Department of Home Affairs. Advanced Electronic Signatures are strongly recommended for strong

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

	authentication, signing, and encryption of electronic communications, transactions, and processes.
--	--

Table 1 Types of Certificates

4.7.2 The South Africa Certification Authority (SACA) is responsible for issuing public key certificates (henceforth referred to as Certifying Authorities or CAs). The CAs, in turn, are responsible for:

- a) issuing Digital Signature Certificates to the end user;
- b) sets policy (as stated in its certification practice statement (CPS), a statement issued by a certification service provider to specify the practices that it employs in generating and issuing digital certificates) on what identification a person must produce in order to obtain a digital certificate; and
- c) in order to maintain security, indicates in a published certificate revocation list those digital certificates that are no longer valid (e.g. revoked, expired or suspended).

4.7.3 A Registration Authority (RA) acts as the verifier for the CA before a Digital Signature Certificate is issued to a requestor. The Registration Authorities process user requests, confirm their identities and induct them into the database.

4.7.4 The guidelines should be used to assist departments in making informed decisions regarding the appropriate use of electronic signatures at each level. Departments must determine the risks and benefits of the available technologies for their specific applications. How an electronic signature works is described in Appendix B.

5. GUIDELINES FOR ELECTRONIC RECORDS

A key issue with electronic signatures is proving that the signature is from the person the signature represents and that the document has not been altered.

5.1. CHARACTERISTICS OF TRUSTWORTHY ELECTRONIC RECORDS

According to the National Archives and Record Service of South Africa Act No. 43 of 1996, the characteristics listed below are used to describe trustworthy records from a records management legal perspective.

5.1.1 Reliability

Record content can be trusted as a full and accurate representation of the transactions, or facts to which it attests and can be depended upon in the course of subsequent transactions.

5.1.2 Authenticity

A record proved to be what it claims to be or to have been created or sent by the person who claims to have created and sent it; assurance of identity.

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

5.1.3 Integrity

Proof that a record is complete and has not been altered.

5.1.4 Usability

A record can be located, retrieved, presented, and interpreted in connection with the transaction that created it.

5.1.5 Signature Intent

The process used to obtain the electronic signature must demonstrate that the user intended to sign the record. Establishing intent includes:

- a) Identifying the purpose of signing the electronic record (could be apparent within the context of the transaction);
- b) Being reasonably certain the signatory knows which electronic record is being signed; and
- c) Providing notice to the signer that their electronic signature is about to be applied to, or associated with, the electronic record (such as an online notice advising the signer that continuing the process will result in an electronic signature).

5.2. ELECTRONIC RECORDS MANAGEMENT²

The process used to conduct electronic transactions must be documented, such as in a formal procedure, and followed consistently.

Electronic Records System Requirements

5.2.1 Consistent

The system processes information in a manner that assures the records they create are credible.

5.2.2 Complete

Contains the content, structure, and context generated by the transaction they documented.

5.2.3 Accurate

Quality control at the input level to ensure the information in the system correctly reflects what is communicated in the transaction.

5.2.4 Preserved

Continue to reflect content, structure, and context within any system by which the records are retained over time.

² Section 13 – Management of public records. National Archives and Records Service of South Africa Act 43 of 1996. Regulation 10 – Management and care of records. National Archives and Records Service of South Africa Act 43 of 1996 - Regulation

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

5.3. NON-REPUDIATION

5.3.1 A property that protects against an individual or entity from denying having performed a particular action related to the data. Non-repudiation services protect the reliability, authenticity, integrity, usability, confidentiality, and legitimate use of the electronically signed document.

Essential elements of a non-repudiation model include:

- a) Evidence of the origin of the message
- b) Evidence of being sent
- c) Evidence of receipt
- d) Timestamp, as needed, by the department of origin
- e) Long-term storage of evidence
- f) Designated adjudicator of prospective disputes

5.3.2 Departments shall maintain adequate documentation of the system design, implementation, use, and migration. The documentation shall include a narrative description of the system, physical and technical characteristics, and any other technical information required to access or process the electronic records.

5.4. PRESERVING ELECTRONIC RECORDS

For a record with an electronic signature to remain trustworthy over the record life cycle, it is necessary to preserve its content, context, and sometimes its structure.

5.4.1 Content

Includes the electronic signature and any associated date or other identifiers, such as organization or title. It provides evidence of a document's reliability and authenticity.

5.4.2 Context

Includes individual identifiers that are not embedded in the content of the record but are used to create and verify the validity of an electronic signature. It provides additional evidence to support the reliability and authenticity of the record.

5.4.3 Structure

Includes the physical and logical format of the record and the relationships between data elements comprising the record. If a department determines it is necessary to maintain the structure of the electronic signature, it must be able to recreate the signature or demonstrate the process used to create the signature.

5.5. STEPS TO ENSURE ELECTRONICALLY-SIGNED RECORDS ARE TRUSTWORTHY:

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

- 5.5.1** Create and maintain documentation of the systems used to create the records that contain electronic signatures.
- 5.5.2** Ensure records that include electronic signatures are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction.
- 5.5.3** Implement standard operating procedures for the creation, use, and management of records that contain electronic signatures and maintain written documentation of those procedures.
- 5.5.4** Create and maintain records according to the documented standard operating procedures.
- 5.5.5** Train department staff in the standard operating procedures.
- 5.5.6** Dispose of records that contain the electronic signatures and the associated records according to the established retention schedule for the department and the National Archives Act No. 43 of 1996.

6. RISK MANAGEMENT OF ELECTRONIC RECORDS

- 6.1.** The purpose of risk management is to identify transaction risk factors that could contribute to the possibility of a challenge being made to the validity or enforceability of the signature. Departments should document the process used to determine transaction risk and maintain a copy of this document in their files for future reference.
- 6.2.** Each potential challenge to the enforceability of an electronic signature, a business analysis, and risk assessment should consider:
 - a) the likelihood of a successful challenge to the validity of the electronic signature; and
 - b) the monetary loss, or another adverse impact, that will result from such a successful challenge to the enforceability of the electronic signature.
- 6.3** A qualitative approach should be taken with respect to the risk analysis. Using such an approach, the risk of a challenge being successful and having a significant impact is defined in more subjective and general terms such as high, moderate, and low. In this regard, qualitative analyses depend more on the expertise, experience, and good judgment of the department managers conducting them than on quantified factors. Department risk management team should be consulted as the department's risk register may need to be updated.

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Moderate	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High

Figure 3 Risk Matrix

6.4 In determining whether a signing process is sufficiently reliable for a particular purpose (see also section 9.4 – The Legal Framework for using Electronic Signatures), department business assessments and risk analyses should consider, at a minimum:

- a) the relationships between the parties;
- b) the value of the transaction;
- c) the risk of unauthorized alteration; and
- d) the likely need for accessible, persuasive information regarding the transaction at some later date.

6.5 In addition, the department should consider any other risks relevant to the particular process. Once these factors are considered separately, the department should consider them together to evaluate the sensitivity of risk for a particular process, relative to the benefit that the process can bring. A Risk Assessment Framework (Appendix C) is proposed for departments. The framework is in addition to the department’s internal risk assessment methodology and the National Treasury Public Sector Risk Management Framework April 2010.

6.6 There are also risks associated with digital signature certificates in that the issued certificate maybe no longer be valid (e.g., revoked, expired or suspended). Departments must verify with the Certifying Authority (CA) issuing certificates to the end-user that:

- a) sets policy (as stated in its certification practice statement (CPS), a statement issued by a certification service provider to specify the practices that it employs in generating and issuing digital certificates) on what identification a person must produce in order to obtain a digital certificate; and
- b) in order to maintain security, indicates in a published certificate revocation list those digital certificates that are no longer valid (e.g. revoked, expired or suspended).
- c) documents signed with valid certificate prior to certificate revocation, expiration or suspension remain valid.

6.7 A Registration Authority (RA) acts as the verifier for the CA before a Digital Signature Certificate is issued to a requestor. The Registration Authorities process user requests, confirm their identities and induct them into the database.

6.8 The overall effectiveness of a given electronic signature process depends on how well the department determined the means to mitigate the risks for particular documents and records to be presented, signed, and archived. The department that carefully considers the risks associated with the types of transactions to be processed can design and implement an electronic signature process that is no riskier than, and in most cases less risky than, the same transaction using paper and a written signature. Doing so provides greater confidence that the electronic signature, when affixed within South Africa, will be admissible into evidence and enforceable.

7. ELECTRONIC SIGNATURE GOVERNANCE

7.1. The governance of electronic signature in a department falls within the Information Security Governance model as proposed in the Information and Communication Technology (ICT) Security Guidelines, Version 1, 09 February 2016. A governance model for ICT security management is shown in Figure 4 below.

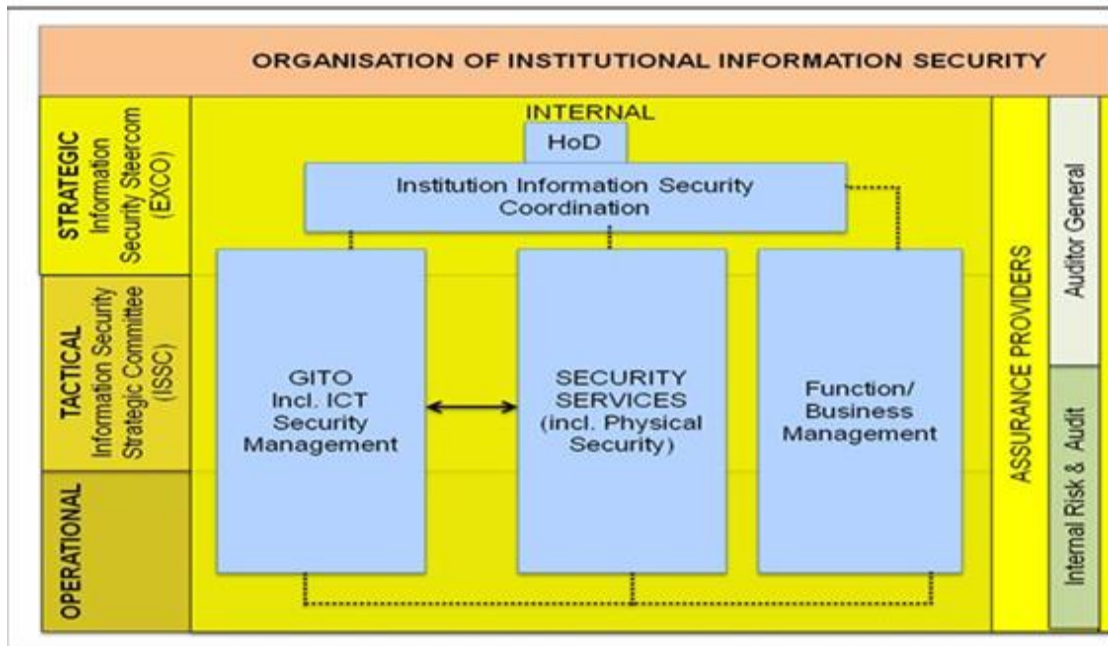


Figure 4 A Governance model for ICT security management

7.2 The roles and responsibility are explained in Appendix E. Where possible the proposed information security structures, roles, and responsibilities should be absorbed within the existing structures, roles, and responsibilities of the department

7.3. The ultimate responsibility for the deployment of an electronic signature solution within a department is vested in the Executive.

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

8. PLANNING OVERVIEW FOR AN ELECTRONIC SIGNATURE PROGRAMME

8.1. BUSINESS ANALYSIS & REQUIREMENTS

As departments gather information on the appropriate use of electronic signatures, they should include a number of subject-matter experts from within their departments. The following subject-matter experts listed below should be considered.

Stakeholder	Information Required
GITO/CIO	Information technology staff should be identified and consulted both for knowledge and guidance on the selection of a particular technology, and also for a thorough understanding of the existing technology architecture of the organization.
Department IT Security	The group should include someone with IT security knowledge and expertise to ensure adequate safeguards are included
Business/Branches	The primary decision a department will make is whether it makes business sense to adopt the use of electronic signatures or records for a particular transaction. Accordingly, knowledgeable members of the business lines impacted by any policy must be included. These members should have an understanding of existing processes and anticipated benefits of using electronic signatures or records
CFO/Finance	To help with the National Treasury requirements and PFMA prescripts
Internal Legal	The question of whether or not a signature or record is required, and whether a proposed electronic signature solution is likely to withstand a challenge should be answered. As this will be accomplished through legal research, appropriate expertise is required
SCM/Procurement	Internal procurement staff should be included so that they are well informed of the department business needs and the impacts. Also, concerns discussed during the decision-making process can be well considered when determining the method of procurement and the resultant contract terms and conditions to ensure that they support the goals of the department.
Records Management	Personnel with knowledge of department record retention and documentation requirements should be included to ensure compliance with these guidelines and other relevant records rules
Internal Audit, Risk and Compliance	Internal Audit should be consulted in order to confirm that the processes are within the prescripts of the Auditor-General requirements. Risk & Compliance to ensure compliance with the department's risk management requirements.
The State Information Technology Agency (SITA).	SITA is the government ICT implementation agency. Besides managing government networks, ICT products are procured through SITA.
Accounting Officer	Approve the use of electronic signatures

Table 2 Stakeholders Information Requirements

8.2. GATHERING REQUIREMENTS

Some areas a department might review include:

Final Version 1.1.0	Guidelines No:2019-1.0.0, Electronic Signatures	Page 15 of 23
-------------------------	---	---------------

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

8.2.1 Existing legislation and regulations.

This area focuses on laws regarding the department's collection and/ or distribution of signatures and records. For any particular document or transaction, the first step should be to determine what the law requires the department to do. For example, is a signature even necessary for a particular transaction? Furthermore, the use of electronic signatures may be prohibited by law. Accordingly, the department should determine whether there is any law that precludes or requires the use of electronic signatures.

8.2.2 Existing department policy and practice.

Current departmental business processes should be reviewed to identify:

- a) potential areas where electronic signatures could be effectively used, and
- b) transactions and documents that are currently electronic in nature.

The department can also begin defining the requirements for those processes and determine the costs associated with each. The department may also put this information into the department policy as the policy is drafted.

8.2.3 Existing records requirements.

The department will need to determine what records retention requirements apply for electronic transactions under consideration, including any retention schedule specific to the department.

8.2.4 Technology capabilities.

The department should have an understanding of adequate and available technological solutions, including electronic records formats and electronic signature methods related to systems currently being used by the department. The department should also focus on the ease-of-use of an electronic signature or records solution, considering the needs and capabilities of both end-users and department personnel.

8.2.5 Current technological architecture.

Electronic signatures and records will also need to fit within the broader departmental Information Technology (IT) environment. In order to make an informed decision about compatibility or interoperability, the department should have a thorough understanding of its current system and where and how new electronic signatures and records can fit within it.

8.3. MAKING ELECTRONIC SIGNATURE DECISION

After the department's stakeholders have identified potential candidates for electronically signed transactions, a determination can be made whether, and in what circumstances, the department will use or accept electronic signatures. For those transactions identified, the department must adopt a policy consistent with the guidelines set forth in this document.

8.3.1 Document the Business Analysis and Risk Assessment (see section 5), documenting the business purpose behind the decisions.

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

8.3.2 Determine which technologies can or cannot fit within the department's current technological architecture. If the current architecture is a barrier to adopting a desirable technology, consider what can or should be changed within the existing architecture to allow for such use.

8.3.3 Begin development of instructions and training materials for end-users and department personnel, particularly if the policy will represent a substantial change in current processes or procedures.

8.4. WRITE A POLICY

Draft the departmental policy reflecting the decisions made in section 8.3. These Guidelines do not specify which electronic signature methods or processes must or should be used. Rather, those decisions are left to departments based on the business assessment and risk analyses they conduct. Departments should consider the following when drafting their policy:

The policy should clearly identify any department specific standards, limitations and processes, including:

8.4.1 Specific technology choices the department has made

8.4.2 Specific transactions the department intends to be completed electronically

8.4.3 Specific groups of constituents that can or cannot use such signatures or records (e.g., the department allows electronic signatures for only certain contracts, or allows electronic filings only for renewal transactions but not an initial application)

8.4.4 Standard processes and methodologies the department intends to follow or use, such as providing users with a document for printing or download as part of the signing process

8.4.5 End-user instructions and other training materials

8.4.6 Update Information Security Policy and Guidelines

8.4.7 Update Electronic Records Management Guidelines (see section 8.5 below)

8.4.8 Incorporate Electronic Signature Governance into the departments' ICT governance

8.5. MANAGING ELECTRONIC RECORDS

8.5.1 Departments on deploying electronic signatures will need to develop a policy on how to manage electronic records.

8.5.2 The policy should be in line with the requirements of the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) on managing Public records. Public records are those created or received in the course of official business and which are kept as evidence of a governmental body's functions, activities, and transactions.

8.5.3 The Electronic Record management methodology adopted must be within the department's internal record management policy, information security policy, and the prescripts of the ECT Act 2002.

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

9. STEPS FOR AN ELECTRONIC SIGNATURES PROGRAMME

Departments should follow these steps to assist them in the implementation and use of electronic signatures.

9.1. IDENTIFY RELEVANT REGULATIONS, POLICIES, AND PROCEDURES

Identify department regulations, policies, and procedures affected by the ECT Act 2002 to ensure the use of electronic signatures is within the prescribed law. The following may be relevant:

- a) Department's Information Security Policy
- b) Minimum Information Security Standards (MISS)
- c) ECT Act 2002
- d) The National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended)
- e) Department's Record Management Policy
- f) Department's Risk Management Policy
- g) PFMA No 1 of 1999
- h) National Cyber Security Policy Framework
- i) POPI Act

9.2. IDENTIFY STAKEHOLDERS/SUBJECT EXPERTS

Identify the stakeholders/subject experts that will be impacted by the electronic signatures programme – see section 8.1.

9.3. EVALUATE CURRENT BUSINESS PROCESS

Evaluate current business processes to determine if a signature is required on a document. Public Service Operations Management Framework: Business Process Management could be used to analyse business processes.

9.4. THE LEGAL FRAMEWORK FOR USE OF ELECTRONIC SIGNATURES

Consider the legal framework for deploying the electronic signature solution. When determining the type of signature that needs to be applied, departments must consider ECT Act Signature decision tree model figure 3 below:

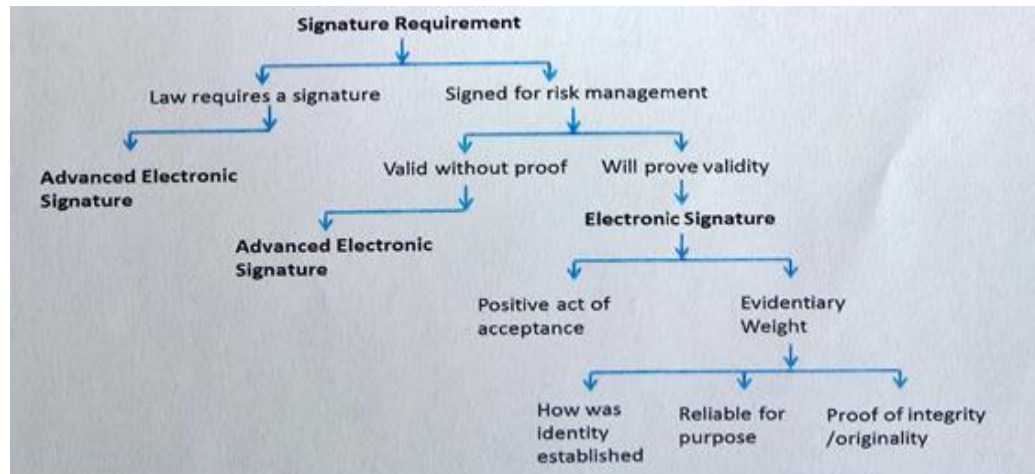


Figure 5 ECT Act Signature decision tree (Adapted from Lawtrust)

- 9.4.1** To understand the decision tree model (figure 5 above), departments must reference section on the type of digital certificates and assurance level – see section 4.7 and Risk Management of Electronic Records - see section 6.
- 9.4.2** Most of the departments are likely to deploy Class 3 digital certificates, as these certificates are suitable for close communities.
- 9.4.3** Where the law requires a signature, that is, valid without proof, only an Advanced Electronic signature can be used.

In summary, the following areas of the ECT Act are of specific importance to deriving benefit from electronic signatures:

9.4.3. 1 Original

An original may be electronic in form, as long as the integrity of the document is assured. This requirement is supported by digital signatures from X.509 digital certificates, which ensures that tampering of the data can be detected.

9.4.3. 2 Evidential Weight

Electronic evidence, including an electronic signature, is subject to assessment for evidential weight.

The assessment will look at:

- a) The reliability of data evidence generation, transmission, and storage
- b) The reliability of the integrity of the data evidence
- c) The method used to identify the parties to the transaction or data evidence
- d) Any other factor that is relevant

This requirement is again easily met by the practices around digital certificates and digital signatures which not only ensures the integrity of data but also creates policy and practices which ensures that the

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

identity of an originator is established formally and in an auditable manner.

9.4.3.3 Advanced electronic signatures

An advanced electronic signature is deemed particularly reliable in law and is prima facie valid i.e. is always assumed to be valid and have been applied correctly so as to shift the burden of proof to the disputing party.

The department's internal legal unit must be consulted for advice on the requirements of the ECT Act 2002.

9.5. THE DECISION TO UTILISE ELECTRONIC SIGNATURE SOLUTION

If a signature is necessary, evaluate each business process in the areas listed below to determine which type of electronic signature meets the business requirements of that document.

9.5.1 Scope of deployment

Determine if the transaction is employee-to-organization, customer-to-organization, organization-to-supplier, etc. Some relationships are inherently more trusted than others. See section 6 Types of Digital Certificates.

9.5.2 Department ICT Technical Infrastructure

An electronic signature solution deployed must complements or fits within the existing technology infrastructure.

9.5.4 Government Regulations

Government Regulations: Determine if any regulations prohibit or restrict the use of electronic signatures for the particular application.

9.6. GOVERNANCE AND SECURITY

9.6.1 The Director-General must approve the deployment of electronic signatures solution.

9.6.2 Departments must engage their internal security unit to facilitate the vetting of the service provider.

9.6.3 Departments do not have to develop separate governance structures but incorporate electronic signature governance into the department's corporate governance of ICT.

9.6.4 The information security policy should be updated to include electronic signature security. The accounting officer must approve the updated policy.

9.6.5 The level of electronic signature selected must ensure the proper level of authentication, confidentiality, integrity, security, and non-repudiation. Departments must consult their internal legal units for advice on the prescripts of the ECT Act 2002.

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

- 9.6.6** Department employees must protect and not disclose or make available their digital signature private key or password to other persons.
- 9.6.7** The department must revoke or send a revocation notice to the certification authority for employees no longer authorized to conduct electronic business on behalf of the department.
- 9.6.8** Departments must document the process used to electronically sign documents and coordinate this process with the department record management policy and guidelines.
- 9.6.9** Each department that uses digital signature technology must establish a digital signature implementation and use policy that:
- a) describes how the department will determine which employees will have a digital signature, the scope of the employee's authority to use the digital signature and for what purposes;
 - b) identifies the roles and responsibilities of issuing digital signatures, letters authorizing the issuance of certificates, procedures to protect digital signatures, and procedures for suspension or revocation of digital signature certificates;
- 9.6.10** Certification Authorities (CA) must provide the following information or meet the following requirements to be authorized to issue digital certificates in South Africa:
- a) Certification Practice Statement (CPS) that documents the practices, procedures, and controls employed by the certification authority.
 - b) Statement of compliance with X.509V3 Certificate.
 - c) Approved (registered) service provider accredited by SAAA

9.7 RISK ASSESSMENT AND MANAGEMENT

In order to implement a digital signature programme which uses the PKI system in the department, the following must be in place:

- 9.7.1** The risk assessment must have been conducted by those who are implementing the project together with the internal ICT security team of a department.
- 9.7.2** The report of the risk assessment should form part of the motivation to implement the program.
- 9.7.3** A comprehensive risk management program must be in place to militate against the identified risks which were identified in the above-mentioned assessment report.
- 9.7.4** Make any necessary revisions regarding the use of signatures to the affected policies e.g., incorporate Electronic Signature policy into the Information Security Policy, and procedures.

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

9.8 UPDATE DOCUMENT RETENTION AND ARCHIVING POLICY

9.8.1 Records created as a result of electronic transactions must be retained according to the department's retention policy, and the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended).

9.8.2 Electronically signed records must contain all the information necessary to reproduce the entire electronic record and associated signatures in a form that permits the person viewing or printing the entire electronic record to verify:

- a) The contents of the electronic record
- b) The method used to sign the electronic record, if applicable
- c) The person(s) signing the electronic record
- d) The date when the signature was executed

9.9 DEVELOP ELECTRONIC SIGNATURE SECURITY AWARENESS TRAINING

Department must develop Electronic Signature Security Awareness guidelines. Department must ensure that employees are trained on:

- a) the use of the application
- b) the implications of its use
- c) the way in which electronically authorised documents should be handled and filed.

9.10 SEEK APPROVAL FROM ACCOUNTING OFFICER

The Executive must approve the use of electronic signature in the National Department. In the Provincial Department or government, the Premier must approve.

Documents to be furnished with the request for approval:

- a) Motivation/Business Case for utilising Electronic Signatures solution
- b) List of documents to be signed electronically
- c) Internal legal advice

GCIO	Electronic Signature Guidelines	DPSA
------	---------------------------------	------

10. REFERENCES

1. Electronic Communications and Transactions Act of 2002
2. LSSA Guidelines Electronic Signatures for South African Law Firms October 2014.pdf [WWW Document], n.d. URL http://www.lssa.org.za/upload/documents/LSSA%20Guidelines_Electronic%20Signatures%20for%20South%20African%20Law%20Firms_October%202014.pdf (accessed 12.7.16).
3. National Cybersecurity Policy Framework - 39475_gon609.pdf [WWW Document], n.d. URL http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf (accessed 12.23.16).
4. National Archives of South Africa Act 43 of 1996 - Act43of1996.pdf [WWW Document], n.d. URL <http://www.gov.za/sites/www.gov.za/files/Act43of1996.pdf> (accessed 12.16.16).
5. New EU regulation for electronic signatures | Insights | DLA Piper Global Law Firm [WWW Document], n.d. DLA Piper. URL <https://www.dlapiper.com/en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures/> (accessed 12.16.16).
6. Electronic signature - Wikipedia [WWW Document], n.d. URL https://en.wikipedia.org/wiki/Electronic_signature (accessed 12.16.16).
7. Public key infrastructure - Wikipedia [WWW Document], n.d. URL https://en.wikipedia.org/wiki/Public_key_infrastructure (accessed 1.4.17).
8. Trust Centre - Powered by the SA Post Office [WWW Document], n.d. URL <https://www.trustcentre.co.za/index.php> (accessed 1.7.17).
9. Global Guide to Electronic Signature Law - adobe-global-guide-electronic-signatures.pdf [WWW Document], n.d. URL <https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf> (accessed 12.7.16).
10. Electronic Signatures and Trust Services - beis-16-15-electronic-signatures-guidance.pdf [WWW Document], n.d. URL https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/beis-16-15-electronic-signatures-guidance.pdf (accessed 12.7.16).
11. 'New EU Regulation for Electronic Signatures | Insights | DLA Piper Global Law Firm'. DLA Piper. Accessed 7 December 2016. <https://www.dlapiper.com/en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures/>.
12. 'What Is PKI (Public Key Infrastructure)? - Definition from WhatIs.com'. *SearchSecurity*. Accessed 23 December 2016. <http://searchsecurity.techtarget.com/definition/PKI>.
13. Guidelines for Usage of Digital Signatures in e-Governance - v1.0 - Guideline-for-digital-signature.pdf [WWW Document], n.d. URL <http://www.daman.nic.in/downloads/2015/Guideline-for-digital-signature.pdf> (accessed 12.16.16).

11. APPENDICES

Appendices attached as a separate document.

Annexure I

POPIA : Supplier Notice and Consent Form

POPIA: SUPPLIER NOTICE AND CONSENT FORM

I confirm that I am duly authorised to sign this consent form.

Name (Print)

Capacity

Signature

Name of Firm

Date



(Hereinafter referred to as “the **Data Subject** “)

A company/organization duly incorporated under the laws of Republic of South Africa, having its
main place of business

At, with

registration number:.....

Preparatory Statement

Whereas the “**Data Subject**” is in agreement with the contents of this Notice and Consent Form and grants SAWS permission to process certain confidential/personal information, for purposes of

whereas the “**Data Subject**” is considering making an offer (the “**Offer**”) to SAWS on a solicited Bid/Tender/RFQ/RFP/RFI, subject to conducting due diligence, as a result of which certain confidential/personal information of the Data Subject may be disclosed to SAWS.

The Data Subject hereby gives consent to the following:

1. Purposes

SAWS will process, including collect, your personal information (as set out in point 2 below) for the following purposes:

- a) strategic sourcing;
- b) procurement;
- c) contract management;
- d) supplier management;
- e) invoice management;
- f) payments;
- g) debt recovery;
- h) fraud prevention; and
- i) supplier discovery.

The provision of personal information is voluntary. However, if you do not provide your personal information, we may not be able to perform the above-mentioned purpose/s.

2. Legal basis for the processing

We process your personal information on the basis that (i) processing information is necessary for pursuing our legitimate interests (according to section 11(1) of the Protection of Personal Information Act, No. 4 of 2013 (“POPIA”)), which lies in achieving the purposes as set out in point 1 above, (ii) processing is necessary to carry out actions for the conclusion or performance of “supply chain management functions” for which you are party (according to section 11(1)(b) of POPIA), or (iii) processing complies with an obligation imposed by law on us (according to section 11(1)(c) of POPIA).

We process the following personal information (for specific natural or juristic person and can be used to identify you or that person):

POPIA: SUPPLIER NOTICE AND CONSENT FORM

- a) Master data
- Name
 - Addresses
 - Contact numbers
 - Email address
 - Other contact details of the supplier
 - Supplier primary contact person's name and contact information
 - Job position and role / qualifications
 - Partner roles of the suppliers needed for invoicing and ordering
 - Identification / company registration number
 - BBBEE status
 - Central Supplier Database number
- b) Accounting and payment information
- VAT & Income tax numbers
 - Tax clearance pin
 - Bank details
 - Bank account type and number
 - Name of the account holder
 - Attachment of confirmation documents
 - Terms of payment
 - Accounting correspondence
- c) Supplier classification
- Category
 - Vendor portfolio
 - Product categories
 - Main product category
 - Additional product categories
 - Vendor category.
- d) Declared conflict or potential conflict of interest
- e) Information on goods and/or services offered by supplier
- quantity and quality of offered goods and/or services
 - other commercial terms of the offer
- f) Contract information
- commercial terms of the contract
 - legal terms of the contract
 - any other contractual documentation
 - information about contract performance and instances of non-performance

POPIA: SUPPLIER NOTICE AND CONSENT FORM

3. Retention periods

Your personal information will only be kept for as long as we reasonably consider necessary for achieving the purposes set out in point 1 above and as is permissible under applicable laws. We will, in any case, retain your personal information for as long as there are statutory retention obligations or potential legal claims are not yet time barred.

4. Law enforcement

We may disclose personal information if required:

- by a subpoena or court order;
- to comply with any law;
- to protect the safety of any individual or the public; and
- to prevent violation of our supplier relation terms.

5. Regulators

We may disclose your personal information as required by law or governmental audit.

6. Sharing

We may share your personal information with:

- other divisions or public entities within the South African Government as the South African Weather Service (SAWS) is a Section 3(a) public entity under the Ministry of Environmental Affairs and is governed by a Board, so as to provide joint content and services like registration, for transactions and customer support, to help detect and prevent potentially illegal acts and violations of our policies, and to guide decisions about our products, services;
- an affiliate, in which case we will seek to require the affiliates to honor this privacy notice;
- our goods or services providers under contract who help provide certain goods or services or help with parts of our business operations, including fraud prevention, bill collection, marketing,
- technology services (our contracts dictate that these goods or services providers only use your information in connection with the goods or services they supply or services they perform for the SAWS and not for their own benefit);
- credit bureaus to report account information, as permitted by law;
- banking partners as required by credit card association rules for inclusion on their list of terminated merchants (in the event that you utilize the services to receive payments and you meet their criteria); and
- other third parties who provide us with relevant services, where appropriate.

7. Suppliers rights

Under applicable law, you have, among others, the rights (under the conditions set out in applicable law):

- (i) to check whether and what kind of personal data we hold about you and to request access to and the right to rectify the information collected
- (ii) in certain circumstances, to object to the processing of personal information, in the prescribed manner, on reasonable grounds relating to your particular situation, unless legislation provides for such processing or to object for the purposes of direct marketing; or

POPIA: SUPPLIER NOTICE AND CONSENT FORM

- (iii) to lodge a complaint with the Information Regulator if they believe that their personal information was not used to the intended purpose. The address of the Information Regulator is Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191.
- (iv) Supplier may withdraw his, her, its Consent so long as they provide SAWS with a “withdrawal of consent notice”, through the Information Officer.
- (v) Supplier may request for correction or deletion of personal information or destruction or deletion of record of personal information.

8. Your obligations

You may only send us your own personal information or the information of another data subject where you have their permission to do so.

9. Security

We take the security of personal information very seriously and always do our best to comply with applicable data protection laws. Our website is hosted in a secure server environment that uses a firewall and other advanced security measures to prevent interference or access from outside intruders. We authorize access to personal information only for those employees who require it to fulfil their job responsibilities. We implement disaster recovery procedures where appropriate.

10. Data Storage

We will try to keep the personal information we collect as accurate, complete, and up to date as is necessary for the purposes defined in this notice. Please note that to better protect you and safeguard your personal information, please inform us of any required corrections to your personal information.

11. Limitation

We are not responsible for, give no warranties, nor make any representations in respect of the privacy policies/notices or practices of any third parties.

12 Enquiries

If you have any questions or concerns arising from this notice and consent form or the way in which we handle personal information, please contact the South African Weather Service Deputy Information Officer:

HEAD OFFICE
1263 Heuwel Road
Centurion
0157
+27 12 367 6000
Email for Head Office: CRS@weathersa.co.za