GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

Provincial Supply Chain Management

INVITATION TO BID

Page 1 of 4

BID NUMBER	GT/GDeG/012/2026
BID DESCRIPTION	THE PROVISION OF EMAIL, ARCHIVING (EXTRACTION, INGESTION, AND STORAGE) AND SECURITY SOLUTION INCLUDING SUPPORT AND MAINTENANCE FOR GAUTENG PROVINCIAL GOVERNMENT(GPG) FOR A PERIOD OF 36 MONTHS

CUSTOMER DEPARTMENT	Gauteng Department of e-Government
CUSTOMER INSTITUTION	Gauteng Department of e-Government

BRIEFING SESSION	**Y**	✔	**N**		**SESSION COMPULSORY**		**Y**	✔	**N**	
					SESSION HIGHLY RECOMMENDED		**Y**		**N**	✔
BRIEFING VENUE	45 Commissioner street, Department of Health				**DATE**	20 March 2026	**TIME**		11:00	
COMPULSORY SITE INSPECTION	**Y**		**N**	✔	**DATE**	N/A	**TIME**		N/A	
SITE INSPECTION ADDRESS	N/A									

TERM AGREEMENT CALLED FOR?	**Y**	✔	**N**		**TERM DURATION**	36 Months

CLOSING DATE	10 April 2026	**CLOSING TIME**	11:00

TENDER BOX LOCATION
75 Fox Street, Marshalltown,Johannesburg

NOTES

THE TENDER BOX IS OPEN From 8:00 till 16:00 during working hours

- Bids / tenders must be deposited in the Tender Box on or before the closing date and time.
- Bids / tenders submitted by fax will not be accepted.
- This bid is subject to the preferential procurement policy framework act, 2000 and the preferential procurement regulations, 2022, the general conditions of contract (gcc) 2010 and, if applicable, any other special conditions of contract.

ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL GPG BID FORMS – (NOT TO BE RE-TYPED) - ALL REQUIRED INFORMATION MUST BE COMPLETED (FAILURE TO DO SO MAY RESULT IN YOUR BID BEING DISQUALIFIED)

THE TENDERING SYSTEM

The Invitation to Bid Pack consists of two Sections (Section 1 and Section 2). These two sections must be submitted separately, clearly marked with the Tender Number and the Section Number.

TRAINING SESSIONS

Non-compulsory **"How to tender"** workshops are held every Wednesday from 10:00 to 13:00. Kindly follow our social media platforms / etenders@gauteng.gov.za (Publications) for the venue of the training.

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

Provincial Supply Chain Management

INVITATION TO BID

PART A
INVITATION TO BID

SUPPLIER INFORMATION					
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
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES OFFERED?	☐ Yes ☐ No [IF YES ENCLOSE PROOF]		ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES OFFERED?	☐ Yes ☐ No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]	

QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS		
IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)?	☐ YES	☐ NO
DOES THE ENTITY HAVE A BRANCH IN THE RSA?	☐ YES	☐ NO
DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA?	☐ YES	☐ NO
DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA?	☐ YES	☐ NO
IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION?	☐ YES	☐ 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.

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

Provincial Supply Chain Management

INVITATION TO BID

TENDER DOCUMETS CAN BE OBTAINED FROM: https://e-tenders.gauteng.gov.za/Pages/Advertised-Open-Tenders.aspx
OR
ALTERNATIVELY SEND AN E-MAIL TO: Tender.admin@gauteng.gov.za

ANY ENQUIRIES REGARDING BIDDING PROCEDURE MAY BE DIRECTED TO:	
DEPARTMENT	Gauteng Department of e-Government
CONTACT PERSON	Sizwe Sibisi
TELEPHONE NUMBER	N/A
FACSIMILE	N/A
E-MAIL ADDRESS	Sizwe.sibisi2@gauteng.gov.za

ANY ENQUIRIES REGARDING TECHNICAL INFORMATION MAY BE DIRECTED TO:	
DEPARTMENT	Gauteng Department of e-Government
CONTACT PERSON	Max Ludwig
TELEPHONE NUMBER	N/A
FACSIMILIE	N/A
E-MAIL ADDRESS	MAX.LUDWIG@gauteng.gov.za

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

Provincial Supply Chain Management

INVITATION TO BID

PART B
TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:

1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. 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, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.

1.4. **THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).**

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 SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.

2.3 APPLICATION FOR 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 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."

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

SIGNATURE OF BIDDER		**DATE**	
CAPACITY UNDER WHICH THIS BID IS SIGNED (Proof of authority must be submitted e.g. company resolution)			

RETURNABLE ATTACHMENT

GAUTENG PROVINCE
e-GOVERNMENT
REPUBLIC OF SOUTH AFRICA

CONSENT FORM TO PROCESS PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT, NO. 4 OF 2013 (POPIA).

The purpose of the POPIA is to protect personal information of individuals and businesses and to give effect to their right of privacy as provided for in the Constitution.
By signing this form, you consent to your personal information to be processed by the Gauteng Department of e-Government and consent is effective immediately and will remain effective until such consent is withdrawn.

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF BIDS

Name & Surname/Company: _____

Residential/Postal or Business Address: _____

_____

Contact number (s): _____

Email address: _____

1. In the furtherance of the Gauteng Department of e-Government (**The Department**) operational requirements and for purposes of complying with its policies, procedures and privacy laws, we may be required to disclose, process and/or further process your personal information provided to us and/or made available by virtue of submission of this bid.

2. For purposes contemplated in paragraph 1, the Department, hereby requests your consent and/or authorisation for the disclosure, processing and/or further processing of any and/or all your personal information as may be necessary for reasons provided in paragraph 1.

3. By signing this Personal Information Processing Consent Form, you hereby grant the Department permission, consent and/or authorisation to disclose, process and further process your personal information within our records, as may be required and/or necessary from time to time.

I, the undersigned, _____ (*INSERT FULL NAME AND SURNAME*) with Identity Number _____, in my personal capacity or acting on behalf of _____ _____(Name of **Company**), confirm that:

4. I have read and understood the contents of this Personal Information Processing Consent form, the details of which have been explained to me and furthermore I understand my right to privacy and the right to have my personal information processed in accordance with the conditions for the lawful processing of personal information.

5. I declare that all my personal information supplied to the Department is accurate, up to date, not misleading and that it is complete in all respects and will be held and/ or stored securely for the purpose for which it was collected and that I will immediately advise the Department of any changes to my Personal Information should any of these details change.

6. I also understand that I have the right to request that my personal information be corrected or deleted, if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully or that the personal information or record be destroyed or deleted if the Department is no longer authorised to retain it.

7. I declare that my personal/the Company's information and/or data may be disclosed, processed and/or further processed by the Department (including its employees, agents, contractors and representatives) and such other third parties contracted with the Department involved in the processing, verification and management of my and/or Company's Personal Information in accordance with the requirements set out in paragraph 1;

8. I accept the data security and protection measures adopted and/or applied by the Department in their retention, disclosure, processing, and further processing of my and/or Company's personal information/data.

9. I accept that the Department may retain any of my personal/the Company information/data as may be required for purposes contemplated in paragraph 1.

10. With my signature below, do hereby give my or the Company's irrevocable consent, and/or authorisation for purposes required and/or detailed in this *Personal Information Processing Consent* form.

Signed at ..... this ..... day of .....20……

…..... ……

Name of data subject/ designated person Signature

…… ……..

Name/Surname/Dept of Responsible Party Signature

Date:

GAUTENG PROVINCE PROVINCIAL TREASURY REPUBLIC OF SOUTH AFRICA	**PROVINCIAL SUPPLY CHAIN MANAGEMENT**	
	INSTRUCTION TO BIDDERS	**Page: 1 of 4**

1.	The INVITATION TO BID Pack is drawn up so that certain essential information should be furnished in a specific manner. Any additional particulars shall be furnished in a separate annexure.
2.	The INVITATION TO BID forms should not be retyped or redrafted, but photocopies may be prepared and used. Additional offers may be made for any item, but only on a photocopy of the page in question or on other forms obtainable from the relevant Department or Institution advertising this BID. Additional offers made in any other manner may be disregarded.
3.	Should the INVITATION TO BID forms not be filled in by means of electronic devices, bidders are encouraged to complete forms in a black ink.
4	Bidders shall check the numbers of the pages and satisfy themselves that none are missing or duplicated. No liability shall be accepted with regards to claims arising from the fact that pages are missing or duplicated.
5	The INVITATION TO BID forms shall be completed, signed and submitted with the bid. SBD 5 (National Industrial Participation Programme Form) will only be added to the INVITATION TO BID pack when an imported component in excess of US $ 10 million is expected.
6	A separate SBD 3.1, SBD 3.2 or SBD 3.3 form (PRICING SCHEDULE per item) shall be completed in respect of each item. Photocopies of this form may be prepared and used or additional copies, (if required) are obtainable from the relevant Department or Institution advertising this BID (not applicable for PANEL of BIDDERS).
7	Firm delivery periods and prices are preferred. Consequently, bidders shall clearly state whether delivery periods and prices will remain firm for the duration of any contract, which may result from this BID, by completing SBD 3.1 (PRICING SCHEDULE per item) (not applicable for PANEL of BIDDERS).
8	If non-firm prices are offered bidders must ensure that a separate SBD 3.2 (Non-Firm Prices per item) is completed in respect of each item for which a non-firm price is offered. Photocopies of this form may be prepared and used or additional copies, (if required) are obtainable from the relevant Department or Institution advertising this BID (not applicable for PANEL of BIDDERS).

9	Where items are specified in detail, the specifications form an integral part of the BID document (see the attached specification) and bidders shall indicate in the space provided whether the items offered are to specification or not (not applicable for PANEL of BIDDERS).
10	In respect of the paragraphs where the items offered are strictly to specification, bidders shall insert the words **"as specified"** (see the attached specification) (not applicable for PANEL of BIDDERS).
11	In cases where the items are not to specification, the deviations from the specifications shall be indicated (see the attached specification).
12	In instances where the bidder is not the manufacturer of the items offered, the bidder must as per SBD 3.1 or SBD 3.2 (PRICING SCHEDULE per item) submit a Letter of Supply from the relevant manufacturer or his supplier (not applicable for PANEL of BIDDERS).
13	The offered prices shall be given in the units shown in the attached specification, as well as in SBD 3.1 or SBD 3.2 (PRICING SCHEDULE per item) (not applicable for PANEL of BIDDERS).
14	With the exception of imported goods, where required, all prices shall be quoted in South African currency. Where bids are submitted for imported goods, foreign currency information must be supplied by completing the relevant portions of SBD 3.1 (PRICING SCHEDULE per item) and SBD 3.2 (PRICING SCHEDULE per item) (not applicable for PANEL of BIDDERS).
15	Unless otherwise indicated, the costs of packaging materials (if applicable) are for the account of the bidder and must be included in the bid price on the (PRICING SCHEDULE per item) (not applicable for PANEL of BIDDERS).
16	Delivery basis (not applicable for PANEL of BIDDERS): a) Supplies which are held in stock or are in transit or on order from South African manufacturers at the date of offer shall be offered on a basis of delivery into consignee's store or on his site within the free delivery area of the bidder's centre, or carriage paid consignee's station, if the goods are required elsewhere. b) Notwithstanding the provisions of paragraph 16(a), offered prices for supplies in respect of which installation / erection / assembly is a requirement, shall include ALL costs on a “delivered on site” basis, as specified on the (PRICING SCHEDULE per item).

17	Unless specifically provided for in the BID document, no bids transmitted by facsimile or email shall be considered.
18	Failure on the part of the bidder to sign any of the INVITATION TO BID forms and thus to acknowledge and accept the conditions in writing or to complete the attached INVITATION TO BID forms, Preference documents, questionnaires and specifications in all respects, may invalidate the bid.
19	Bids should preferably not be qualified by the bidder's own conditions of bid. Failure to comply with these requirements (i.e. full acceptance of the General Conditions of Contract or to renounce specifically the bidder's own conditions of bid, when called upon to do so, may invalidate the bid.
20	In case of samples being called for together with the bid, the successful bidder may be required to submit pre-production samples to the South African Bureau of Standards (SABS) or such testing authority as designated at the request of the relevant Department concerned. Unless the relevant Department decides otherwise, pre-production samples must be submitted within thirty (30) days of the date on which the successful bidder was requested to do so. Mass production may commence only after both the relevant Department and the successful bidder have been advised by the SABS that the pre-production samples have been approved.
21	Should the pre-production samples pass the inspections / tests at the first attempt, the costs associated with the inspections / tests will be for the account of the relevant Department. If the SABS or such testing authority as designated do not approve the pre-production samples, but requires corrections / improvements, the costs of the inspections / tests must be paid by the successful bidder and samples which are acceptable in all respects must then reach the SABS or such testing authority as designated within twenty-one (21) days of the date on which the findings of the SABS or such testing authority as designated were received by the successful bidder. Failure to deliver samples within the specified time and to the required standards may lead to the cancellation of the intended contract.
22	In case of samples being called for together with the bid, the samples must be submitted together with the bid before the closing time and date of the BID, unless specifically indicated otherwise. Failure to submit the requested sample(s)before the closing time and date of the BID may invalidate the bid.
23	In cases where large quantities of a product are called for, it may be necessary for the relevant item to be shared among two (2) or more suppliers.

24	In cases where the relevant Department or Institution advertising this BID may deem it necessary, a formal contract may be entered into with the successful bidder, in addition to a Letter of Acceptance and / or purchase order being issued.
25	If any of the conditions on the BID forms are in conflict with any special conditions, stipulations or provisions incorporated in the bid invitation, such special conditions, stipulations or provisions shall apply.
26	This BID is subject to the General Conditions of Contract and re-issues thereof. Copies of these conditions are obtainable from any office of the Gauteng Provincial Government (GPG).
27	Each bid must be submitted in a separate, sealed envelope on which the following must be clearly indicated: • NAME AND ADDRESS OF THE BIDDER; • THE BID (GT) NUMBER; AND • THE CLOSING DATE. The bid must be deposited or posted; • To the address as indicated on SBD1 and to reach the destination not later than the closing time and date; **OR** • deposited in the tender box as indicated on SBD1 before the closing time and date.
28	The Gauteng Provincial Government has become a member and as such a key sponsor of the Proudly South African Campaign. GPG therefore would like to procure local products of a high quality, produced through the practise of sound labour relations and in an environment where high environmental standards are maintained. In terms of the Proudly South African Campaign South African companies are encouraged to submit interesting and innovative achievements in the manufacturing field (if relevant to this BID) – including information on new products, export achievements, new partnerships and successes and milestones.
29	Compulsory GPG Contract: It is a mandatory requirement that successful bidder/s (to whom a tender is awarded) sign a GPG Contract upon award of any given contract.

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

PROVINCIAL SUPPLY CHAIN MANAGEMENT

POINT SYSTEM

BID NUMBER	GT/GDeG/012/2026	**CLOSING DATE**	10 April 2026
VALIDITY OF BID	90 Days	**CLOSING TIME**	11:00

The goods / services are required by the Customer Department / Institution, as indicated on SBD 01.

This BID will be evaluated on the basis of the under noted point system, as stipulated in the Preferential Procurement Policy Framework Act (Act number 5 of 2000).

POINT SYSTEM

The applicable preference point system for this tender is the 90/10 preference point system.	✔
The applicable preference point system for this tender is the 80/20 preference point system.	
Either the 90/10 or 80/20 preference point system will be applicable in this tender	

TYPE OF CONTRACT (COMPLETED BY PROJECT MANAGER)

SERVICE BASED	**Y**	✔	**N**		**SERVICE BASED**	**Y**	✔	**N**		**VALUE BASED**	**Y**	✔	**N**	
VALUE BASED	**Y**	✔	**N**											
QUANTITY BASED	**Y**		**N**	✔										
TERM BASED	**Y**	✔	**N**											

GAUTENG PROVINCE PROVINCIAL TREASURY REPUBLIC OF SOUTH AFRICA	**Provincial Supply Chain Management**	
	Compulsory Briefing Session	Page 1 of 1

COMPULSORY BRIEFING DECLARATION OF ATTENDANCE

BID NUMBER	GT/GDeG/012/2026		
BID DESCRIPTION	THE PROVISION OF EMAIL, ARCHIVING (EXTRACTION, INGESTION, AND STORAGE) AND SECURITY SOLUTION INCLUDING SUPPORT AND MAINTENANCE FOR GAUTENG PROVINCIAL GOVERNMENT(GPG) FOR A PERIOD OF 36 MONTHS		
CLOSING DATE	10 April 2026	**CLOSING TIME**	11:00

The goods / services are required by the Customer Department / Institution, as indicated on form SBD1.

CUSTOMER DEPARTMENT	Gauteng Department of e-Government						
CUSTOMER INSTITUTION							
BRIEFING SESSION	**Y**	☑	**N**	☐	**DATE** 20 March 2026	**TIME**	11:00 am
VENUE	45 Commissioner street, Department of Health						

I/We hereby declare that I/we attended the compulsory briefing session to understand the requirements of the Gauteng Provincial Government to supply all or any of the supplies and/or to render all or any of the services described in the attached Bid documents, on the terms and conditions and in accordance with the specifications stipulated in the Bid documents.

I, THE UNDERSIGNED (NAME)

CERTIFY THAT THE INFORMATION FURNISHED AT THE BRIEFING SESSION WAS UNDERSTOOD.

BIDDER OR ASSIGNEE(S) NAME		**POSITION**		**SIGN**		**DATE**	
FULL COMPANY NAME							
GPG OFFICIAL NAME		**POSITION**		**SIGN**		**DATE**	

END USER STAMP

GAUTENG PROVINCE PROVINCIAL TREASURY REPUBLIC OF SOUTH AFRICA	PROVINCIAL SUPPLY CHAIN MANAGEMENT	
	BIDDER'S DISCLOSURE	Page: 1 of 3

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 interest 1 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.

GAUTENG PROVINCE PROVINCIAL TREASURY REPUBLIC OF SOUTH AFRICA	PROVINCIAL SUPPLY CHAIN MANAGEMENT	
	BIDDER'S DISCLOSURE	Page: 2 of 3

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 consortium 2 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.

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.

GAUTENG PROVINCE PROVINCIAL TREASURY REPUBLIC OF SOUTH AFRICA	PROVINCIAL SUPPLY CHAIN MANAGEMENT	
	BIDDER'S DISCLOSURE	**Page: 3 of 3**

3.5 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.

3.6 There have been no consultations, communications, agreements or 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.

3.7 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 the Bidder**	

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

PROVINCIAL SUPPLY CHAIN MANAGEMENT

EVALUATION METHODOLOGY PROCESS

EVALUATION METHODOLOGY

- Bidders must complete Compulsory Documents and attach it to their Bid Document failing which the tender shall not be considered for further evaluation.
- Points will be awarded in accordance with the Preferential Procurement Policy Framework Act (PPPFA)

STAGE 1

CRITERIA FOR FUNCTIONALITY	
1. Advanced email security	59
2. The provision of an on-premise GPG owned email	
and archiving, e-discovery software solution.	14
3. Extracting and ingesting email archives into a GPG owned archive	8
4. Technical Training	6
5. Customer Support and Service Level agreements.	12
6. Project Plan	10
7.Team Skills set	11
8.Experience (References)	50
	170

NOTE: Bidders who fail to meet the above minimum requirements (Stage 1) shall be automatically eliminated and will not be considered for further evaluation.

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

PROVINCIAL SUPPLY CHAIN MANAGEMENT

EVALUATION METHODOLOGY PROCESS

STAGE 2

CRITERIA FOR PRICE AND PREFERENCE POINTS (SPECIFIC GOALS)	POINTS
Bid Price	90
Preference Points (Specific Goals)	10
TOTAL	100

SPECIFIC GOALS SHALL BE ALLOCATED AS FOLLOWS:

	POINTS ALLOCATED
SPECIFIC GOALS	
1.Women owned companies	5
2.Companies owned by youth	5
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

***It is the responsibility of the bidder to complete the relevant form (SBD 6.1) and submit it with this BID to the relevant office to qualify for the preference points.**

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

PROVINCIAL SUPPLY CHAIN MANAGEMENT

EVALUATION METHODOLOGY PROCESS

BIDDERS JOB CREATION ANALYSIS

Company Name		**Date Established**	

	Permanent	**Temp**	**SA Citizens**	**Other**	**Comments**
Staff compliment at Establishment of Enterprise					
Current staff compliment					
Number of jobs to be created if Bid is successful					

The successful bidder may be audited during the course of the contract to verify the above information.

Comments to include:

- If Job Creation is direct (by your own company) or indirect (by your source of supply)
- Where the jobs created for employees that were in existing positions or unemployed? (Net Job Creation)

NOTE: Job Creation should adhere to all applicable RSA Legislation and Regulations.

THIS SECTION IS FOR OFFICE USE ONLY						
Observations	**Initial Job Count**	**Job Creation Potential**	**1st Quarter**	**2nd Quarter**	**3rd Quarter**	**4th Quarter**
Year 1						
Year 2						
Year 3						
Year 4						
Year 5						

GAUTENG PROVINCE
e-GOVERNMENT
REPUBLIC OF SOUTH AFRICA

TERMS OF REFERENCE

FOR

THE PROVISION OF

EMAIL, ARCHIVING (EXTRACTION, INGESTION, AND STORAGE) AND SECURITY SOLUTION INCLUDING SUPPORT AND MAINTENANCE FOR GAUTENG PROVINCIAL GOVERNMENT(GPG) FOR A PERIOD OF 36 MONTHS

1. BACKGROUND

The Gauteng Provincial Government (GPG) has embarked on a digital transformation journey to modernize the public sector. As part of this digital transformation journey, the province has invested in various digital platforms.

The Email Security and Archiving Solution focuses on email security, the extraction and ingestion of archived mail, the provision of an email archiving and retrieval tool.

Below is a technical specification for implementing a comprehensive Email Security and Archiving Solution, with particular focus on data extraction and ingestion from existing archiving environments into a GPG archiving solution. As vital data is often kept solely in email systems, organizations need reliable archiving to maintain integrity, meet regulations, and enable quick access, all while controlling storage costs and complexity.

The GPG has identified the need to optimize its email operations. The GPG relies heavily on email to drive business operations, management efficiency, improve communication, and staff productivity. To meet business goals, the GPG has implemented an email security and archiving solution.

The following services are currently provided.

1.1 General email services.

1.1.1 The general inbound, outbound, and internal email service that is being utilized by GPG is Microsoft 365. The total number of email users is 36300.

1.1.2 The mailbox sizes are governed by the Microsoft 365 rules.

1.1.3 The average growth of email has been 5% year on year.

1.2 E-Gov provides first line email support and maintenance.

1.3 Advanced email security.

1.3.1 All emails enter the Service Providers email security solution.

1.3.2 Each email with its attachments are comprehensively tested and checked through advanced threat protection for any suspected/suspicious security breaches. These emails are either blocked and removed if they are deemed to be compromised or are tested and declared clear of any suspected/suspicious material before they are delivered to Microsoft 365.

1.4 Compliant archiving & recovery, Proof of delivery, Chains of custody are retained. End user archive access.

1.4.1 All emails that are pasted in the Microsoft 365 environment are also copied into an email archiving solution.

1.4.2 The archived mail will have proof of delivery the chains of custody must be retained, and end users can access email the archived email. The archiving is Based on Microsoft SQL database.

1.4.3 Solution has e-Discovery capabilities.

1.5 Continuity (BCP planning).

1.5.1 Business continuity planning is provided for all archived mail.

2. CUSTOMER AND STAKEHOLDERS

2a. Customer

2.1 Gauteng Department of e-Government

2b. Stakeholders

a. Office of the Premier
b. Gauteng Department of Education
c. Gauteng Department of Roads and Transport
d. Gauteng Department of Infrastructure Development
e. Gauteng Department of Human Settlements
f. Gauteng Department of Health
g. Gauteng Department of Social Development
h. Gauteng Department of Sports, Arts, Culture and Recreation
i. Gauteng Department of Agriculture and Rural Development
j. Gauteng Department of Economic Development
k. Gauteng Department of Community Safety
l. Gauteng Provincial Treasury
m. Gauteng Department of Co-operative Governance and Traditional Affairs
n. Gauteng Department of Environment

2c. SCOPE OF WORK

There are 3 distinctive solutions that are required for the email security and Archiving solution. These are:

2.1 Advanced email security.

2.2 The provision of a GPG owned email and archiving and retrieval tool.

2.3 Extracting and ingesting email archives into a GPG owned archive.

2.1 Advanced email security

The bidder must provide a comprehensive, multi-layered email security and data protection solution for all incoming and outgoing emails, both internal and external, across the Gauteng Provincial Government (GPG) environment, combining advanced technical controls with real-time, behaviour-driven human risk reduction.

The solution must be a robust, scalable and compliant email security solution that provides real-time scanning and analysis of incoming and outgoing emails, both internal and external to detect and block malware, ransomware, phishing, spear phishing, provide data loss protection from insider threats, advanced business email compromise and effectively prevent zero-day threats using artificial intelligence (AI), machine learning (ML), and signature-based detection.

The solution must ensure business continuity and compliance with South African data protection and public sector regulations.

Every email with its attachments that comes into the system must be first subjected to all the security checks and if all checks are passed, each email with its attachments will be transferred to Microsoft 365 exchange online and to the on-premise GPG archive solution.

The solution must include:

(a) Advanced Email Security and Threat Protection

i. An Advanced Email Security and Threat Protection capability that protects GPG users from advanced email-borne threats, including phishing, malware, ransomware, and targeted attacks.
ii. Business continuity and compliance with South African data protection and public sector regulations.
iii. Advanced Threat Protection: Multi-layered threat defense and sandboxing that provides real-time inspection and filtering of all inbound and outbound email traffic for protection against phishing, malware, ransomware and zero-day attacks, leveraging global threat intelligence and AI/ML.
iv. Impersonation & Brand Protection: Detects and blocks advanced business email compromise, CEO/CFO fraud and domain spoofing, with warning banners and brand monitoring.

v. URL and Attachment Protection: Enforce granular policies for attachment and URL protection, including real-time rewriting and scanning of links and files.
vi. Spam & Malware Filtering: Industry-leading detection engines that block over 99% of spam and malware with near-zero false positives.
vii. Data Leak Prevention (DLP): Granular, policy-driven controls to prevent unauthorized sharing of sensitive data, with automated alerts and blocking.
viii. Secure Messaging: Encrypted, policy-based secure messaging for confidential communications, accessible via a secure portal.
ix. Continuity & Resilience: Cloud-based email continuity that ensures uninterrupted access during outages, with seamless failover and failback.
x. Centralized Management & Reporting: Unified console for policy management, real-time dashboards for threat analytics, policy enforcement, and compliance monitoring, customizable reports, and permanent audit trails.
xi. Integration with Microsoft 365: Deep, Application Programming Interface (API-enabled) integration for consistent policy enforcement, Single Sign-On (SSO), and directory sync.
xii. No Infrastructure Required: 100% cloud-native, with no server or client installations, ensuring rapid deployment and scalability for large, distributed environments.

(b) Data Protection & Compliance

i. Data loss prevention and insider threats by detecting, investigating and responding to insider risks and data exfiltration events across endpoints, cloud and email, ensuring that sensitive GPG data is not leaked or misused.
ii. Reduction of insider risk by educating users in real time when risky or non-compliant behaviors are detected, fostering a culture of security awareness.
iii. Extend insider risk detection and response to email communications within Microsoft Office 365, ensuring that sensitive data is not exfiltrated via email.
iv. Monitor and protect sensitive data stored and shared via cloud storage, ensuring compliance with data governance and security policies.
v. Ensure compliance with data protection regulations and internal retention/classification policies.
vi. Comprehensive Data Risk Monitoring: Monitor and analyze file movements, sharing, and transfers across endpoints, cloud storage, and email, detecting unauthorized or suspicious exfiltration of sensitive data.
vii. Contextual Risk Scoring: Provide real-time context-rich alerts and automated response actions for policy violations, including blocking, quarantining, or alerting security teams.
viii. Behavior-Triggered Microlearning: Offer targeted, in-the-moment security training to users based on observed risky actions, such as unauthorized file sharing or external transfers to educate staff on secure data handling and reduce risky behaviors.

ix. Monitoring and Compliance Reporting: Deliver detailed audit trails and reporting for all monitored activities, supporting investigations, compliance, and litigation on hold requirements.

x. Seamless Integration: Integrate seamlessly with Microsoft Office 365 and OneDrive, ensuring comprehensive coverage of GPG's cloud collaboration environment.

(c) Authentication & Identity Security

i. Protect GPG's domains from being spoofed or abused in phishing attacks, ensuring only authorized senders can use official GPG email domains and improving trust in government communications.

ii. Achieve compliance with Domain-based Message Authentication, Reporting & Conformance (DMARC) standards.

iii. Visibility: Provide full visibility into all email senders using GPG domains, distinguishing between legitimate and fraudulent sources.

iv. Reporting and Analytics: Generate actionable DMARC reports and analytics to monitor authentication status and identify sources failing DMARC, Sender Policy Framework (SPF), or DomainKeys Identified Mail (DKIM) checks.

v. Policy Enforcement: Enable policy enforcement to reject or quarantine unauthenticated emails, reducing the risk of phishing and domain impersonation.

vi. DMARC Managed Service: The Managed Service must include expert guidance for DMARC policy implementation, ongoing monitoring, and remediation support to accelerate DMARC adoption and maximize protection.

(d) Monitoring & Alerts

i. A centrally managed, unified, efficient and auditable platform for managing, monitoring, and reporting on all aspects of email security and controls, threat intelligence, data protection and human risk that effectively enables proactive risk reduction, regulatory compliance and operational efficiency across all departments.

ii. Unified Cloud-Native Platform: Must deliver a single, integrated cloud platform for email security, data protection and compliance, human risk management and reporting that streamlines administration, policy management and reporting for all security and compliance functions.

iii. Human Risk Command Center: Must uniquely aggregate technical and behavioral risk signals into a centralized dashboard, providing real-time visibility into both system and user-driven risks. This must enable GPG security teams to prioritize interventions and measure risk reduction outcomes.

iv. Automated, Actionable Reporting: Must provide automated, customizable reports on threats, compliance, user behavior and policy enforcement. Reports must be audit-ready and scheduled or generated on demand, supporting both operational oversight and regulatory requirements.

v. Seamless Integration: Must integrate natively with Microsoft 365, Azure AD, Security Information and Event Management (SIEM), and other security and compliance tools, ensuring consistent policy enforcement and data flow without the need for complex connectors or additional infrastructure.

vi. Granular Role-Based Access: Administrators must be able to assign granular permissions for reporting, policy management and incident response, supporting GPG's need for departmental autonomy and centralized oversight.

vii. Real-Time Analytics and Alerts: Must provide an analytics engine that delivers real-time dashboards and alerts for threats, incidents and compliance gaps, enabling rapid response and continuous improvement.

viii. Comprehensive Audit Trails: All actions, policy changes and user activities must be logged in tamper-proof audit trails, supporting investigations, legal holds and compliance audits.

(e) Email Incident Response

i. Enable swift response to evolving threats through rapid detection, investigation and remediation of email-borne threats post-delivery, minimizing the impact of attacks and reducing manual workload for GPG IT and security teams.

ii. Automated Threat Remediation: Automate identification, analysis and removal of malicious or unwanted emails from user inboxes post-delivery, across the entire GPG environment.

iii. Incident Response Workflows: Provide incident response workflows, including investigation, containment, and remediation actions, with full audit trails.

iv. Threat Intelligence Integration: Integrate with real-time threat intelligence feeds and user-reported phishing mechanisms to accelerate detection and response.

v. Reporting and Analytics: Support reporting and analytics on incident trends, response times, and outcomes.

(f) Unified Risk Command Centre

i. Blocks not only email borne cyber threats but also proactively reduces cyber risk stemming from human behavior.

ii. Unified Risk Dashboard: The solution must provide a Human Risk Command Centre that offers a single pane of glass for all human risk signals, allowing GPG security teams to prioritize, automate, and track interventions across the organization.

iii. Scalability & Simplicity: The solution must support 36,300 users plus 5% annual growth with centralized, cloud-native management and minimal administrative overhead.

iv. Automated Policy Enforcement: The solution must provide for policies that adapt dynamically based on user risk profiles, always ensuring the right level of protection for each user.
v. Integrated Incident Response: The solution must provide real-time detection and escalation of risky behaviors, with automated controls for high-risk users.
vi. Dynamic Human Risk Scoring: The solution must provide real-time, behavior-based risk scoring for every user, aggregating signals from email, endpoint, and third-party tools to enable targeted interventions for the most at-risk users.
vii. Proactively Reduce Human Risk: The solution must not only block email borne cyber threats but also measurably reduce human-driven risk by identifying, scoring, and remediating risky user behaviors in real time.

(g) User Cyber Awareness & Training

i. Reduce the risk of security breaches caused by human error by equipping all GPG employees with the knowledge and skills to recognize and respond appropriately to cyber threats, including phishing, social engineering, and data handling risks.
ii. Enhance user engagement and awareness regarding email security threats and best practices and foster a culture of security awareness and compliance across all departments.
iii. Support targeted communication and training initiatives across all GPG departments.
iv. Behavioral Analytics & Nudges: The platform must leverage behavioral insights and risk signals by continuously monitoring user interactions with email, identifying patterns of risky behavior and triggering automated, context-aware, targeted and adaptive micro-training interventions to GPG employees based on their demonstrated risk profile and behavior.
v. Multi-Channel Interventions: Nudges and training must be delivered via email, collaboration tools to maximize user engagement and learning retention.
vi. Engaging, Modern Content: The platform must provide highly engaging, short-form training modules and videos, designed by industry professionals, that cover a wide range of cybersecurity topics such as phishing, password hygiene, data privacy, and safe remote working. Content must be updated regularly to address emerging threats and compliance requirements.
vii. Phishing Simulation and Testing: The platform must include automated phishing simulations to test GPG employee susceptibility to real-world attacks and leverage such results to tailor future training and provide measurable improvements in user awareness and behavior.

viii. Risk Scoring and Analytics: The platform must continuously assess individual and organizational risk through behavioral analytics, training completion rates and phishing test results. Administrators must receive behavioral feedback via actionable dashboards and reports to identify high-risk users and departments, track progress and demonstrate compliance to drive sustained risk reduction.

ix. Seamless Integration: The platform must integrate with existing email and identity platforms, including Microsoft 365, for automated user provisioning, single sign-on and centralized management.

x. Unified Behavioral Analytics Engine: All behavioral data and interventions must be fed into the Human Risk Command Centre, enabling coordinated, organization-wide risk reduction strategies.

xi. Policy and Compliance Alignment: Training modules and reporting must be aligned with GPG's regulatory and policy requirements, supporting audit readiness and ongoing compliance with national and provincial information security standards.

Solution Summary Table: Email Security Solution Capabilities and Outcomes

Requirement/Capability	Solution Capability	Outcome/Benefit
Advanced Threat Protection	Multi-layered protection leverages AI/ML, threat intelligence, and sandboxing to defend against phishing, malware, ransomware, and zero-day attacks—across inbound and outbound email.	Blocks evolving and sophisticated threats, prevents business disruption, and protects sensitive data from compromise.
Impersonation & Brand Protection	The solution must detect and block impersonation attempts including BEC, CEO/CFO fraud using header analysis, domain similarity, warning banners alert users to suspicious messages and brand monitoring.	Protects against financial fraud, reputational harm, and data loss caused by identity deception, while increasing user vigilance against targeted attacks.
Spam & Malware Filtering	The solution must provide advanced filtering engines that	Maintains productivity, minimizes risk of

Requirement/Capability	Solution Capability	Outcome/Benefit
	block spam, viruses, and malware with high accuracy and low false positives, and quarantines suspicious emails for admin/user review.	infection, and reduces time spent managing unwanted email to support a safe and efficient work environment.
Data Leak Prevention (DLP)	The solution must provide policy-driven DLP scans on email content/attachments, automatically blocks or alerts on sensitive data leakage, and integrates with risk scoring for adaptive controls.	Prevents unauthorized data sharing, supports compliance and reduces regulatory and legal exposure from accidental or intentional data leaks.
Secure Messaging	The solution must provide a cloud-based secure messaging portal with policy-based encryption, automatic triggers for sensitive content and seamless experience for internal/external recipients.	Ensures confidentiality and integrity for sensitive communications, enables compliant information sharing and supports audits and legal holds.
Continuity & Resilience	The solution must provide cloud-native email continuity service that enables automatic failover and access to email during outages or attacks, with real-time monitoring and seamless integration.	Guarantees uninterrupted business operations, fulfils business continuity planning requirements and minimizes downtime impact on productivity.
Real-Time Human Risk Scoring	A platform that continuously manages and evaluates human risk, user behaviours	Enables proactive identification and remediation of high-risk users,

Requirement/Capability	Solution Capability	Outcome/Benefit
	and security signals to assign dynamic risk scores to individuals, GPG departments as listed above.	reducing human error as a threat vector and allowing targeted security interventions.
Unified Risk Command Center	A centralized Risk Command Center that aggregates behavioural analytics, risk scores, and incident data, providing a single interface for security teams to monitor, prioritize, and respond across the entire environment.	Delivers full visibility, enables efficient risk management, and supports compliance by integrating human and technical risks into one actionable dashboard.
Adaptive, Continuous Training	The solution must provide automated, micro-learning interventions triggered by user behaviour and risk level, integrated with the centralized Risk Command Centre for feedback and tracking.	Builds a culture of security, lowers organizational risk, and ensures ongoing compliance by keeping users engaged and informed with relevant, timely education.
Behavioural Awareness Training Nudges (In-Moment)	The solution must deliver context-aware, real-time awareness training nudges now risky actions including suspicious link clicks,	Immediately educates users, modifies risky behaviour at point-of-risk, and lowers repeat offenses, allowing for more

Requirement/Capability	Solution Capability	Outcome/Benefit
	unsafe data sharing is detected.	effective user training than traditional, periodic training.
Centralized Management & Reporting	The solution must provide a unified, cloud-based admin console that caters for policy management, real-time dashboards, customizable reporting, audit trails and integration with Microsoft 365 and other security tools.	Streamlines administration, enhances visibility, supports compliance/audit needs, and reduces complexity and overhead for IT/security teams.
No Infrastructure Required	The solution must be 100% cloud-native solution with no hardware/software to install or manage and integrates with existing email platforms via secure APIs and directory sync.	Rapid, non-disruptive deployment and scaling for 36,300 users plus 5% annual growth, reduces IT burden and enables secure, consistent user experience across the organization.

The solution must be hosted and managed in compliance with South African data residency and public sector requirements, ensuring data sovereignty, privacy, and business continuity.

2.2 The provision of an on-premise GPG owned email and archiving, e-discovery software solution.

Introduction

Email archiving refers to the systematic process of preserving email communications in a secure, indexed, and retrievable digital format. Email archiving focuses on long-term preservation of emails and their attachments while ensuring the original version of each

message remains unaltered and verifiable. Modern email archiving solutions create a centralized repository that captures every message, attachment, and thread in a manner that supports regulatory compliance, legal discovery, and knowledge retention initiatives.

Solution requirements

i. The bidder must provide an on-premises GPG owned email and archiving, e-discovery software solution that operates on a real-time journaling-based capture mechanism that collects all email traffic, inbound, outbound, and internal, ensuring a complete record of GPG email communications. This comprehensive capture approach prevents data gaps and ensures the archive represents a tamper-evident record of all email transactions.

ii. Provide, end-to-end encryption of archived emails both at rest and in transit is required.

iii. The solution must provide retention policies to be applied at multiple levels, organization, group, mailbox, or folder, providing granular control over data lifecycle management. These policies ensure compliance with regulatory requirements while automatically purging data that no longer needs to be retained, reducing storage costs and legal risk.

iv. The solution must have the capabilities to purge/dispose of email records manually or automatically as determined by the authorized officials.

v. The solution must have the ability to place emails under legal hold for the duration of an investigation or litigation, overriding standard retention policies.

vi. The solution must contain advanced search and eDiscovery methods for fast, full-text search with advanced filters (metadata, sender, recipient, keywords, date) for efficient retrieval and legal discovery.

vii. The capability to secure export of archived emails in standard formats (Personal Storage Table (PST), Email Massage Format (EML), Mailbox (MBOX) for migration, audits, or regulatory requests must exist within the solution.

viii. The solution must be seamlessly integrated with various email platforms, including Microsoft Office 365, Exchange, and other hosted environments, providing consistent archiving regardless of the underlying email infrastructure.

ix. The solution must employ advanced deduplication techniques that eliminate redundant copies of attachments and messages, significantly reducing storage requirements without compromising completeness or integrity.

x. Provision of access controls is a requirement. The access controls must be role-based and policy driven access with the inclusion of Multi-factor Authentication (MFA). Access to emails may be required for litigation or investigation purposes.

xi. The solution must provide a web portal allowing users to access their own archived email, restoring emails and attachments to their live mailbox if required. Users may not delete or remove any emails or attachments from the archive.

xii. The on-premise GPG owned email and archiving, e-discovery software solution must have a full set of monitoring, reporting, and analytics tools.

xiii. The solution must have the ability to provide permanent audit trials to retain a complete record of what actions are performed on records, including deletion. What records management metadata is included in the audit trail can be specified.

xiv. The solution must provide mechanisms for ensuring the integrity of the email archive and that only email records that are eligible for purging may be removed by the authorized officials.

2.3 Extracting and ingesting email archives into a GPG owned archive.

Introduction

The extraction and ingestion of all archived data from the source achieves to the destination archive must be part of the bidder's proposal and the data must be made available in a format that is compatible and usable in Microsoft 365 Exchange Online.

Email data Archives.

The existing archived emails that must be extracted and ingested from the current archive system to the new archive system are as follows:

i. The GPG Email archive that is currently being held within Mimecast Limited. The size of this archive is 292TB of uncompressed data.
ii. The GPG Email archive that is currently being held within Brilliantel Telecommunication (PTY) Ltd. The size of this archive is 250TB of uncompressed data.
iii. The total size of the archived data as at the 2025-09-29 is 542TB of uncompressed data.
iv. The existing Microsoft 365 exchange online mail.

Data Extraction Methodology

The bidder must provide the methodology for the extraction of email and attachments from the exiting archives provided above. The methodology must include an extraction scope, the data sources and the verification of all emails and attachments extracted.

Data Ingestion Methodology

i. The bidder must provide the methodology for the ingestion of extracted emails and attachments from the exiting archives provided above. The ingestion methodology transforms extracted email data into a structured format suitable for loading into the target archiving system. This process involves multiple stages of data validation, transformation, and indexing to ensure the ingested data meets the requirements of the archive environment and solution. A well-defined ingestion methodology is critical for maintaining data integrity and ensuring the usability of the archived content.

ii. During ingestion, all files should undergo comprehensive virus scanning using regularly updated signature databases to prevent malware introduction into the archive environment. Infected files should be quarantined or removed from the processing stream to maintain system security. Following virus scanning, the system should generate cryptographic hash values for each file using industry-standard algorithms such as SHA-256. These hash values serve as unique identifiers that facilitate deduplication and provide verification of data integrity throughout the retention period.

iii. Once the email archive has been extracted from the source archive and ingested into on premise centralized archiving platform, it is fully content indexed and stored with a tamper-proof, digitally encrypted signature and timestamp for establishing retention periods at the object level.

iv. The archived email data extraction will be ingested to the centralized archiving platform and will need to be migrated within a period of 12 months.

NOTE:

a. Bidder must provide details of how each of the services will be delivered and clearly articulate the outcomes of each of the services required.

b. All inbound outbound email must be provided through a single point of entry, and detailed solution architecture must be provided indicating the single point of entry.

c. There must be a highly secure and resilient on-premise GPG owned email and archiving, e-discovery software solution.

d. E-Gov will provide the hardware and disaster recovery that is required to host the GPG owned email and archiving, e-discovery software solution.

e. E-Gov reserves the right to choose and accept a solution that is the most suitable and cost effective for the Gauteng Provincial Government.

3. TECHNICAL TRAINING

Technical and support training must be provided for GPG officials on the products and solutions that will be deployed/ implemented by the bidder.

Advanced email security

3.1 One official from each Department (15) will need to be trained in first list support for the provision of advanced email security.

3.2 The email administrators from e-Gov (2) will be required to be certified to enable to provide 3rd Line support for advanced email security.

The provision of an on-premise GPG owned email and archiving, e-discovery software solution.

3.3 One official from each Department (15) will need to be trained in first line support for the provision of email and archiving, e-discovery software solutions.

3.4 The email administrators from e-Gov (2) will be required to be certified to enable to provide 3rd Line support for email and archiving, e-discovery software solution.

3.5 The directorate (Records management team 12) will need training on utilizing the archiving, e-discovery software solution with a specific focus on the management of email archives which will include the purging, disposing, and deleting of email records and attachments that no longer fall within the ambit of the email retention and disposal policy.

3.6 The concept of train-the-trainer must us used to provide training to all GPG employees who have email accounts on how to use the web-portal to search for and copy archived emails and attachments which they may require. There must be 3 officials from each GPG department who must be trained as trainers to be able to train other users on how to use the web-portal. This equates to 44 trainers.

4. CUSTOMER SUPPORT AND SERVICE LEVEL AGREEMENTS

A comprehensive service level agreement must be drawn up which must include support and maintenance for the duration of the contract. Support and maintenance is required for the following:

4.1 Advanced email security

- 24/7 Support: support desk, multi-language support, and escalation procedures.
- Service Level Agreements: Clearly defined performance, uptime, and response targets, with financial penalties for missed commitments.
- Maintain, and enhance the email security solution including supporting GPG technical users when required.
- Weekly and monthly reporting. As per section (h) of advanced email security.
- Active alert monitoring
- Conduct an audit of the email security environment bi-annually and implement remedial recommendations where necessary.

4.2 The provision of a GPG owned email and archiving and retrieval tool.

- 24/7 Support: support desk, multi-language support, and escalation procedures.
- Service Level Agreements: Clearly defined performance, uptime, and response targets, with financial penalties for missed commitments.
- Maintain, and enhance the GPG owned email and archiving and retrieval tool including supporting GPG technical users when required.
- Weekly and monthly reporting, as per section (xi) of GPG owned email and archiving and retrieval tool.

4.3 Extracting and ingesting email archives into a GPG owned archive.

- The bidder must provide comprehensive verification solution for the extraction and ingestion of email records and attachments into the archiving and retrieval tool.

- Reporting is required for the email records that are extracted and ingested into the GPG owned email and archiving and retrieval tool.

5. PROJECT PLAN

Provide a comprehensive plan of the following milestones and timelines that must be ingestion of archived emails.

5.1 The project plan must be in line with the scope of work.

5.2 Solution Requirements and Blueprint.

5.3 Provide the design, deployment/ Implementation, solution testing, of the user Interface for the advanced email security, the deployment of the GPG owned email and archiving and retrieval tool, and the extracting and ingesting of email archives into a GPG owned archive.

5.4 Include user acceptance testing for the solutions to be deployed.

5.5 Training documentation.

5.6 Go-live technical support for the solutions to be deployed.

6. EXPERIENCE

Enterprise Support Experience:

Advanced email security

6.1 The bidder must allocate a dedicated team for support with at least 5 years' experience in supporting enterprise advanced email security platforms and cloud services.

6.2 The bidder must provide the makeup of the team which clearly articulates the 5 years' experience.

6.3 The Bidder must provide (5) contactable references for the provision of advanced email security platforms.

The provision of an on-premise GPG owned email and archiving, e-discovery software solution.

6.4 The bidder must allocate a dedicated team for support with at least 5 years' experience in supporting email and archiving, e-discovery software solutions.

6.5 The bidder must provide the makeup of the team which clearly articulates the 5 years' experience.

6.6 The Bidder must provide (3) contactable references for the provision of advanced email security platforms.

Extracting and ingesting email archives into a GPG owned archive.

6.7 The bidder must furnish demonstrable proof of their capability to extract data from Mimecast and Brilliantel Telecommunication (PTY) Ltd and ingest data into the archived software solution proposed in this specification. This proof comprise of a minimum of one customer attestation or official documentation from the relevant Original Equipment Manufacturer (OEM) Provider, clearly detailing the migration timeline and the volume of archived data successfully migrated.

7. TIME FRAME

The duration of the contract is 36 months/3 years, which will include the following:

- Advanced email security.
- The provision of a GPG owned email and archiving and retrieval tool.
- Extracting and ingesting email archives into a GPG owned archive.

The bidder must note that the implementation of the email archiving service must be completed and operational within a maximum of 12 months from the award date which will form part of the 36-month legal agreement. The project will be implemented in a modular approach in line with the project plan.

GENERAL CONDITIONS

RFP Pack

General conditions are stipulations to establish the general risks, liabilities, and obligations of the contract in the various documents which make up the RFP pack.

The use of subcontractors

No part of the work covered by the contract may be let or sub-let to persons including companies, unless authorized in writing by the Accounting Officer in which Preferential Procurement Regulations 2017, section 12 must be applied, which authority, if granted, shall not in any way absolve the contractor of any liability which might result from the contract.

Total Cost of Ownership

The bidder is required to submit a detailed breakdown of all costs associated with the initial development of the solution, including any future costs associated with maintenance and support. In addition, the bidder/s should submit different types of billing models available for the solution.

the right to audit (Assurance)

E-Gov reserves the right to audit the deployment of archived email and security services.

8. EVALUATION METHODOLOGY

THE STAGED APPROACH WHICH WILL BE APPLIED IN THE EVALUATION OF BIDS

Stage one will be the evaluation of bids on **Administration Compliance** and **Technical Evaluation**

During these stages, the bidder/s that do not meet the minimum required threshold per each stage of evaluation will be disqualified and will not be considered for further evaluation.

Stage Two evaluation will be based on Price and Preference points only.

- Price = 90 points.
- Preference = 10 points.

STAGE 1B: ADMINISTRATIVE MANDATORY COMPLIANCE

A mandatory letter from both Mimecast and Brilliantel committing to grant permission to the successful bidder to extract and ingest data into the archived software solution proposed in this specification.

Bidder/s that fail to meet the above requirement shall be disqualified.

Bidder/s must complete, sign, and submit all pages of Tender Bid Documents Section 1 (RFP- Request for Proposal) and Section 2 (Price Schedule – Professional Services).

Bid Commitment and Declaration of Interest Form must be complete, signed and submitted by the Bidder (RFP 04).

Bidder/s must submit original compulsory briefing session certificate that is signed and stamped.

If there is a share of services between Bidder i.e., Joint Venture/Consortium, all participating parties must submit the following supporting documents:

Service Agreement stating the roles and the share percentage of the value of the project undertaken and signed by all parties,

NB: Bidder/s that fail to meet required criteria stipulated under Administrative Mandatory Compliance shall not be considered for further evaluation.

OTHER REQUIRED DOCUMENTS:

Tax Clearance Certificate Pin code.

Bidder/s are required by the Department of e-GOV to provide Audited Annual Financial statements for the past three years.

Proof of registration with the National Treasury Supplier Database (CSD).

Certified copy of Company and Intellectual Property Combination (CIPC) Certificate.

STAGE 1B: TECHNICAL EVALUATION

- A total of 170 points is allocated for stage 1B.

The threshold for this part of the evaluation is **128** points (75%); any bidder who fails to meet this minimum requirement shall be deemed non-responsive and eliminated from any further evaluation.

AREA	COMMENTS`	POINTS

1. Advanced email security	**(a) Advanced Email Security and Threat Protection** i. An Advanced Email Security and Threat Protection capability that protects GPG users from advanced email-borne threats, including phishing, malware, ransomware, and targeted attacks (1 point). ii. Business continuity and compliance with South African data protection and public sector regulations. (1 point). iii. Advanced Threat Protection: Multi-layered threat defense and sandboxing that provides real-time inspection and filtering of all inbound and outbound email traffic for protection against phishing, malware, ransomware and zero-day attacks, leveraging global threat intelligence and AI/ML (1 point). iv. Impersonation & Brand Protection: Detects and blocks advanced business email compromise, CEO/CFO fraud and domain spoofing, with warning banners and brand monitoring (1 point). v. URL and Attachment Protection: Enforce granular policies for attachment and URL protection, including real-time rewriting and scanning of links and files (1 point). vi. Spam & Malware Filtering: Industry-leading detection engines that block over 99% of spam and malware with near-zero false positives (1 point). vii. Data Leak Prevention (DLP): Granular, policy-driven controls to prevent unauthorized sharing of sensitive data, with automated alerts and blocking (1 point). viii. Secure Messaging: Encrypted, policy-based secure messaging for confidential	**12**

	communications, accessible via a secure portal (1 point). ix. Continuity & Resilience: Cloud-based email continuity that ensures uninterrupted access during outages, with seamless failover and failback (1 point). x. Centralized Management & Reporting: Unified console for policy management, real-time dashboards for threat analytics, policy enforcement, and compliance monitoring, customizable reports, and permanent audit trails (1 point). xi. Integration with Microsoft 365: Deep, API-enabled integration for consistent policy enforcement, SSO, and directory sync (1 point). xii. No Infrastructure Required: 100% cloud-native, with no server or client installations, ensuring rapid deployment and scalability for large, distributed environments (1 point).	
	(b) Data Protection & Compliance i. Data loss prevention and insider threats by detecting, investigating and responding to insider risks and data exfiltration events across endpoints, cloud and email, ensuring that sensitive GPG data is not leaked or misused (1 point). ii. Reduction of insider risk by educating users in real time when risky or non-compliant behaviors are detected, fostering a culture of security awareness (1 point). iii. Extend insider risk detection and response to email communications within Microsoft Office 365, ensuring that sensitive data is not exfiltrated via email (1 point). iv. Monitor and protect sensitive data stored and shared via cloud storage, ensuring	**10**

	compliance with data governance and security policies. (1 point). v. Ensure compliance with data protection regulations, and internal retention/classification policies (1 point). vi. Comprehensive Data Risk Monitoring: Monitor and analyze file movements, sharing, and transfers across endpoints, cloud storage, and email, detecting unauthorized or suspicious exfiltration of sensitive data (1 point). vii. Contextual Risk Scoring: Provide real-time context-rich alerts and automated response actions for policy violations, including blocking, quarantining, or alerting security teams (1 point). viii. Behavior-Triggered Microlearning: Offer targeted, in-the-moment security training to users based on observed risky actions, such as unauthorized file sharing or external transfers to educate staff on secure data handling and reduce risky behaviors (1 point). ix. Monitoring and Compliance Reporting: Deliver detailed audit trails and reporting for all monitored activities, support investigations, compliance, and litigation on hold requirements (1 point). x. Seamless Integration: Integrate seamlessly with Microsoft Office 365 and OneDrive, ensuring comprehensive coverage of GPG's cloud collaboration environment. (1 point).	
	(c) Authentication & Identity Security i. Protect GPG's domains from being spoofed or abused in phishing attacks, ensuring only authorized senders can use official GPG	**6**

	email domains and improving trust in government communications (1 point). ii. Achieve compliance with DMARC (Domain-based Message Authentication, Reporting & Conformance) standards (1 point). iii. Visibility: Provide full visibility into all email senders using GPG domains, distinguishing between legitimate and fraudulent sources (1 point). iv. Reporting and Analytics: Generate actionable DMARC reports and analytics to monitor authentication status and identify sources failing DMARC, SPF, or DKIM checks (1 point). v. Policy Enforcement: Enable policy enforcement to reject or quarantine unauthenticated emails, reducing the risk of phishing and domain impersonation (1 point). vi. DMARC Managed Service: The Managed Service must include expert guidance for DMARC policy implementation, ongoing monitoring, and remediation support to accelerate DMARC adoption and maximize protection (1 point).	
	(d) Mail Flow Monitoring & Control i. A centrally managed, unified, efficient and auditable platform for managing, monitoring, and reporting on all aspects of email security and controls, threat intelligence, data protection and human risk that effectively enables proactive risk reduction, regulatory compliance and operational efficiency across all departments. (1 point) ii. Unified Cloud-Native Platform: Must deliver a single, integrated cloud platform for email security, data protection and compliance, human risk management and reporting that streamlines administration, policy	**8**

	management and reporting for all security and compliance functions. (1 point) iii. Human Risk Command Center: Must uniquely aggregate technical and behavioral risk signals into a centralized dashboard, providing real-time visibility into both system and user-driven risks. This must enable GPG security teams to prioritize interventions and measure risk reduction outcomes (1 point), iv. Automated, Actionable Reporting: Must provide automated, customizable reports on threats, compliance, user behavior and policy enforcement. Reports must be audit ready and scheduled or generated on demand, supporting both operational oversight and regulatory requirements (1 point). v. Seamless Integration: Must integrate natively with Microsoft 365, Azure AD, SIEM, and other security and compliance tools, ensuring consistent policy enforcement and data flow without the need for complex connectors or additional infrastructure (1 point). vi. Granular Role-Based Access: Administrators must be able to assign granular permissions for reporting, policy management and incident response, supporting GPG's need for departmental autonomy and centralized oversight (1 point). vii. Real-Time Analytics and Alerts: Must provide an analytics engine that delivers real-time dashboards and alerts for threats, incidents and compliance gaps, enabling rapid response and continuous improvement (1 point).	

	viii. Comprehensive Audit Trails: All actions, policy changes and user activities must be logged in tamper-proof audit trails, supporting investigations, legal holds and compliance audits (1 point).	
	(e) Email Incident Response i. Enable swift response to evolving threats through rapid detection, investigation and remediation of email-borne threats post-delivery, minimizing the impact of attacks and reducing manual workload for GPG IT and security teams (1 point). ii. Automated Threat Remediation: Automate identification, analysis and removal of malicious or unwanted emails from user inboxes post-delivery, across the entire GPG environment (1 point). iii. Incident Response Workflows: Provide incident response workflows, including investigation, containment, and remediation actions, with full audit trails (1 point). iv. Threat Intelligence Integration: Integrate with real-time threat intelligence feeds and user-reported phishing mechanisms to accelerate detection and response (1 point). v. Reporting and Analytics: Support reporting and analytics on incident trends, response times, and outcomes (1 point).	**5**
	(f) Unified Risk Command Centre i. Blocks not only email borne cyber threats but also proactively reduces cyber risk stemming from human behavior (1 point). ii. Unified Risk Dashboard: The solution must provide a Human Risk Command Centre that offers a single pane of glass for all human risk signals, allowing GPG security teams to prioritize, automate, and track interventions across the organization (1 point).	**7**

	iii. Scalability & Simplicity: The solution must support 36,300 users with centralized, cloud-native management and minimal administrative overhead (1 point). iv. Automated Policy Enforcement: The solution must provide for policies that adapt dynamically based on user risk profiles, always ensuring the right level of protection for each user (1 point). v. Integrated Incident Response: The solution must provide real-time detection and escalation of risky behaviors, with automated controls for high-risk users (1 point). vi. Dynamic Human Risk Scoring: The solution must provide real-time, behavior-based risk scoring for every user, aggregating signals from email, endpoint, and third-party tools to enable targeted interventions for the most at-risk users (1 point). vii. Proactively Reduce Human Risk: The solution must not only block email borne cyber threats but also measurably reduce human-driven risk by identifying, scoring, and remediating risky user behaviors in real time (1 point).	
	(g) User Cyber Awareness & Training i. Reduce the risk of security breaches caused by human error by equipping all GPG employees with the knowledge and skills to recognize and respond appropriately to cyber threats, including phishing, social engineering, and data handling risks (1 point). ii. Enhance user engagement and awareness regarding email security threats and best practices and foster a culture of security awareness and compliance across all departments (1 point). iii. Support targeted communication and training initiatives across all GPG departments (1 point).	**11**

	iv. Behavioral Analytics & Nudges: The platform must leverage behavioral insights and risk signals by continuously monitoring user interactions with email, identifying patterns of risky behavior and triggering automated, context-aware, targeted and adaptive micro-training interventions to GPG employees based on their demonstrated risk profile and behavior (1 point). v. Multi-Channel Interventions: Nudges and training must be delivered via email, collaboration tools to maximize user engagement and learning retention (1 point). vi. Engaging, Modern Content: The platform must provide highly engaging, short-form training modules and videos, designed by industry professionals, that cover a wide range of cybersecurity topics such as phishing, password hygiene, data privacy, and safe remote working. Content must be updated regularly to address emerging threats and compliance requirements (1 point). vii. Phishing Simulation and Testing: The platform must include automated phishing simulations to test GPG employee susceptibility to real-world attacks and leverage such results to tailor future training and provide measurable improvements in user awareness and behavior (1 point). viii. Risk Scoring and Analytics: The platform must continuously assess individual and organizational risk through behavioral analytics, training completion rates and phishing test results. Administrators must receive behavioral feedback via actionable dashboards and reports to identify high-risk users and departments, track progress and demonstrate compliance to drive sustained risk reduction (1 point).	

	ix. Seamless Integration: The platform must integrate with existing email and identity platforms, including Microsoft 365, for automated user provisioning, single sign-on and centralized management (1 point). x. Unified Behavioral Analytics Engine: All behavioral data and interventions must be fed into the Human Risk Command Centre, enabling coordinated, organization-wide risk reduction strategies (1 point). xi. Policy and Compliance Alignment: Training modules and reporting must be aligned with GPG's regulatory and policy requirements, supporting audit readiness and ongoing compliance with national and provincial information security standards (1 point).	
Total		**59**
2. The provision of an on-premise GPG owned email and archiving, e-discovery software solution.	**Solution requirements** i. The bidder must provide an on-premises GPG owned email and archiving, e-discovery software solution that operates on a real-time journaling-based capture mechanism that collects all email traffic, inbound, outbound, and internal, ensuring a complete record of GPG email communications. This comprehensive capture approach prevents data gaps and ensures the archive represents a tamper-evident record of all email transactions (1 point). ii. Provide, end-to-end encryption of archived emails both at rest and in transit is required (1 point). iii. The solution must provide retention policies to be applied at multiple levels, organization,	

	group, mailbox, or folder, providing granular control over data lifecycle management. These policies ensure compliance with regulatory requirements while automatically purging data that no longer needs to be retained, reducing storage costs and legal risk (1 point). iv. The solution must have the capabilities to purge/dispose of email records manually or automatically as determined by the authorized officials (1 point). v. The solution must have the ability to place emails under legal hold for the duration of an investigation or litigation, overriding standard retention policies (1 point). vi. The solution must contain advanced search and eDiscovery methods for fast, full-text search with advanced filters (metadata, sender, recipient, keywords, date) for efficient retrieval and legal discovery (1 point). vii. The capability to secure export of archived emails in standard formats (PST, EML, MBOX) for migration, audits, or regulatory requests must exist within the solution (1 point). viii. The solution must be seamlessly integrated with various email platforms, including Microsoft Office 365, Exchange, and other hosted environments, providing consistent archiving regardless of the underlying email infrastructure (1 point). ix. The solution must employ advanced deduplication techniques that eliminate redundant copies of attachments and messages, significantly reducing storage requirements without compromising completeness or integrity (1 point).	

	x. Provision of access controls is a requirement. The access controls must be role-based and policy driven access with the inclusion of Multi-factor Authentication (MFA). Access to emails may be required for litigation or investigation purposes (1 point). xi. The solution must provide a web portal allowing users to access their own archived email, restoring emails and attachments to their live mailbox if required. Users may not delete or remove any emails or attachments from the archive (1 point). xii. The on-premise GPG owned email and archiving, e-discovery software solution must have a full set of monitoring, reporting, and analytics tools (1 point). xiii. The solution must have the ability to provide permanent audit trials to retain a complete record of what actions are performed on records, including deletion. What records management metadata is included in the audit trail can be specified (1 point). xiv. The solution must provide mechanisms for ensuring the integrity of the email archive and that only email records that are eligible for purging may be removed by the authorized officials. (1 point).	
Total		**14**
3. Extracting and ingesting email archives into a GPG owned archive	**Email data Archives.** **Data Extraction Methodology** i. The bidder must provide the methodology for the extraction of email and attachments	

	from the exiting archives provided above. The methodology must include an extraction scope, the data sources and the verification of all emails and attachments extracted (4 points). **Data Ingestion Methodology** i. The bidder must provide the methodology for the ingestion of extracted emails and attachments from the exiting archives provided above. The ingestion methodology transforms extracted email data into a structured format suitable for loading into the target archiving system. This process involves multiple stages of data validation, transformation, and indexing to ensure the ingested data meets the requirements of the archive environment and solution. A well-defined ingestion methodology is critical for maintaining data integrity and ensuring the usability of the archived content (1 point). ii. During ingestion, all files should undergo comprehensive virus scanning using regularly updated signature databases to prevent malware introduction into the archive environment. Infected files should be quarantined or removed from the processing stream to maintain system security. Following virus scanning, the system should generate cryptographic hash values for each file using industry-standard algorithms such as SHA-256. These hash values serve as unique identifiers that facilitate de-duplication and provide	

	verification of data integrity throughout the retention period (1 point). iii. Once the email archive has been extracted from the source archive and ingested into on premise centralized archiving platform, it is fully content indexed and stored with a tamper-proof, digitally encrypted signature and timestamp for establishing retention periods at the object level (1 point). iv. The archived email data extraction will be ingested to the centralized archiving platform and will need to be migrated within a period of 12 months (1 point).	
Total		**8**
4. Technical Training	Technical and support training must be provided for GPG officials on the products and solutions that will be deployed/ implemented by the bidder. **Advanced email security** i. One official from each Department (15) will need to be trained in first list support for the provision of advanced email security (1 point). ii. The email administrators from e-Gov (2) will be required to be certified to enable 3rd Line support for advanced email security (1 point).	

	The provision of an on-premise GPG owned email and archiving, e-discovery software solution. i. One official from each Department (15) will need to be trained in first line support for the provision of email and archiving, e-discovery software solutions (1 point). ii. The email administrators from e-Gov (2) will be required to be certified to enable to provide 3rd Line support for email and archiving, e-discovery software solution (1 point). iii. The directorate (Records management team 12) will need training on utilizing the archiving, e-discovery software solution with a specific focus on the management of email archives which will include the purging, disposing, and deleting of email records and attachments that no longer fall within the ambit of the email retention and disposal policy (1 point). iv. The concept of train-the-trainer must us used to provide training to all GPG employees who have email accounts on how to use the web-portal to search for and copy archived emails and attachments which they may require. There must be 3 officials from each GPG department who must be trained as trainers to be able to train other users on how to use the web-portal. This equates to 44 trainees (1 point).	
Total		**6**

5. Customer Support and Service Level agreements.	**Advanced email security** i. 24/7 Support: support desk, multi-language support, and escalation procedures (1 point). ii. Service Level Agreements: Clearly defined performance, uptime, and response targets, with financial penalties for missed commitments (1 point). iii. Maintain, and enhance the email security solution including supporting GPG technical users when required. iv. Weekly and monthly reporting. As per section (h) of advanced email security (1 point). v. Active alert monitoring (1 point). vi. Conduct an audit of the email security environment bi-annually and implement remedial recommendations where necessary (1 point). **The provision of a GPG owned email and archiving and retrieval tool.** i. 24/7 Support: support desk, multi-language support, and escalation procedures (1 point). ii. Service Level Agreements: Clearly defined performance, uptime, and response targets, with financial penalties for missed commitments (1 point). iii. Maintain, and enhance the GPG owned email and archiving and retrieval tool including supporting GPG technical users when required (1 point).	

	iv. Weekly and monthly reporting, as per section (xi) of GPG owned email and archiving and retrieval tool (1 point). **Extracting and ingesting email archives into a GPG owned archive.** i. The bidder must provide comprehensive verification solution for the extraction and ingestion of email records and attachments into the archiving and retrieval tool (1 point). ii. Reporting is required for the email records that are extracted and ingested into the GPG owned email and archiving and retrieval tool (1 point).	
Total		**12**
6. Project Plan	Provide a comprehensive plan of the following milestones and timelines that must be ingestion of archived emails. i. The project plan must be in line with the scope of work (1 point). ii. Solution Requirements and Blueprint (1 point). iii. Provide the design, deployment/ Implementation, solution testing, of the user Interface for the advanced email security, the deployment of the GPG owned email and archiving and retrieval tool, and the extracting and ingesting of email archives into a GPG owned archive (1 point). iv. Include user acceptance testing for the solutions to be deployed (1 point). v. Training documentation (1 point). vi. Demonstration of the Go-live technical support for the solutions to be deployed (5 point).	

Total		**10**
Team Skills set	A letter from a bidder stating profiles of a dedicated team with relevant expertise in the required field for support with at least 5 years' experience in supporting enterprise advanced email archiving, security platforms and cloud services (11 point).	
Total		**11**
7. Experience (References)	**Enterprise Support Experience**: **Advanced email security** The bidder must: - provide at least **five (5)** contactable references evidencing capability to the provide advanced email security platforms. **(Total 5 points)** for each letter. These reference letters must be: • Contactable reference • It must be on an official letterhead of the company for which the work was done. • It must clearly specify the duration and the quality of service which was rendered. • Signed and Dated by the company for which the work was done. • No emails can be used as reference letters. - 5 references and more (5) - 4 references (4) - 3 references (3) - Less than 3 refences no points will be allocated. **The provision of an on-premises GPG owned email and archiving, e-discovery software solution.** The bidder must: - provide at least **five (5)** contactable references evidencing capability in provision of an on-premise GPG owned email and	

	archiving, e-discovery software solution at least 5 years' experience. **(Total 5 points)** for each letter. These reference letters must be: • Contactable reference • It must be on an official letterhead of the company for which the work was done. • It must clearly specify the duration and the quality of service which was rendered. • Signed and Dated by the company for which the work was done. • No emails can be used as reference letters. - 5 references and more (5) - 4 references (4) - 3 references (3) - Less than 3 refences no points will be allocated.	
Total		**50**
TOTAL		**170**

STAGE TWO: PREFERENTIAL PROCUREMENT/PRICE

The second stage of evaluation will be on the (90/10 preference point system in terms of which points are awarded to bidders, where 10 points are allocated for preference and 90 points for price only.

The contract will be awarded in terms of the Preferential Procurement Policy Framework Act, (Act 5 of 2000) and Preferential Procurement Regulation 2022.
Price = 90 points
Preference = 10 points

Specific goal	Points	Evidence
Women owned companies	5	BBBEE and full CSD report

Companies owned by youth	5	BBBEE and full CSD report
	10	

Failure on the part of a bidder 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.

GAUTENG PROVINCE
PROVINCIAL TREASURY
REPUBLIC OF SOUTH AFRICA

Provincial Supply Chain Management

Financial Statements

Submission of Financial Statements

The latest financial statements for the last two years are required (except if it is a new or a dormant entity)

a) Financial statements must be signed by the auditor (in the case of companies) or the accounting officer (in the case of close corporations) the owner (in case of sole proprietors). Signatures must be on the accounting officer's / auditors report on the auditor's /accounting officer's letterhead.

b) Financial statements must be signed by the member/s (in the case of close corporations) or by the director/s (in the case of companies.)

c) In bids where consortia/joint ventures/sub-contractors and partnerships are involved, all bidders must submit their financial statements.

d) If it is a new or dormant entity an opening set of financial statements must be submitted. A letter from the auditor (in the case of companies) or the accounting officer (in the case of close corporations) stating that the entity has not yet traded must be submitted.

e) In cases where an entity has operated for a period less than a year the Management Accounts Report for the period in operation must be submitted signed accordingly as stated in paragraph (a) and (b) of this document.

f) In cases where the entity has operated for a period more than a year but less that two years, then the financial statement for the first year of operation signed accordingly as per paragraph (a) and (b) of this document must be submitted.

GAUTENG PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

GAUTENG ETHICS & ANTI CORRUPTION

INTEGRITY PACT FOR BUSINESSES

GAUTENG PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

GAUTENG ETHICS & ANTICORRUPTION

FIGHTING CORRUPTION, PROMOTING INTEGRITY

1. INTRODUCTION

This agreement is part of the tender document, which shall be signed and submitted along with the tender document. The Chief Executive Officer of the bidding company or his/her authorised representative shall sign the integrity pact. If the winning bidder has not signed this integrity pact during the submission of the bid, the tender/proposal shall be disqualified.

2. OBJECTIVES

Now, therefore, the Gauteng Provincial Government and the Bidder agree to enter into this pre-contract agreement, hereinafter referred to as an integrity pact, to avoid all forms of corruption by following a system that is fair, transparent, and free from any influence/unprejudiced dealings before, during and after the currency of the contract to be entered, with a view to:

2.1 Enable the Gauteng Provincial Government to obtain the desired contract at a reasonable and competitive price in conformity to the defined specifications of the works, goods and services; and

2.2 Enable bidders to abstain from bribing or any corrupt practice to secure the contract by assuring them that their competitors will refrain from bribing and other corrupt practices and the Gauteng Provincial Government will commit to preventing corruption, in any form by their officials by following transparent procedures.

3. GOVERNANCE

3.1 The integrity pact seeks to ensure that both parties comply with all applicable provincial, national, continental, and international laws and regulations regarding fair competition and anti-corruption.

4. ENVIRONMENT

4.1 The integrity pact requires that both parties comply with all applicable environmental, health, and safety regulations.

5. PROTECTION OF INFORMATION

5.1 The integrity pact seeks to ensure that both parties undertake to protect the confidentiality of information. Each party, when given access to confidential information as part of the business relationship should not share this information with anyone unless authorised.

6. REPUTATION

6.1 The Gauteng Provincial Government wants to work with bidders who are proud of their reputation for fair dealing and quality delivery.

6.2 The Gauteng Provincial Government wants to ensure that working with government is reputation enhancing for the supplier.

6.3 The Gauteng Provincial Government expects bidders/suppliers to be protective of government's reputation, and ensure that neither they, nor any of their partners or subcontractors, bring government to disrepute by engaging in any act or omission which is reasonably likely to diminish the trust that the public places in government.

6.4 The Gauteng Provincial Government further requires its bidders/suppliers to always adhere to ethical conduct even outside their contractual obligation with the Gauteng Provincial Government.

7. VALUES OF THE GAUTENG PROVINCIAL GOVERNMENT

7.1 The value system of the Gauteng City Region is shown below:

GAUTENG CITY REGION VALUES SYSTEM	
CORE VALUES	**ETHICAL VALUES**
Patriotism Purposefulness Team focused Integrity Accountability Passionate Activism	Integrity Accountability Dignity Transparency Respect Honesty

7.2 The Gauteng Provincial Government commits to ensure that the values system is embedded into the day-to-day operations of its institutions.

8. COMMITMENTS OF THE GAUTENG PROVINCIAL GOVERNMENT

The Gauteng Provincial Government commits itself to the following:

8.1 The GPG commits that its officials will at all times conduct themselves in accordance with Treasury Regulations 16A.8[1], copy of which is attached marked Annexure A, and that:

8.1.1 The GPG is committed to doing business with integrity and proper regard for ethical business practices.

8.1.2 The GPG hereby undertakes that no official of the GPG, connected directly or indirectly with the contract will demand, take a promise for or accept, directly or through

[1] Government Notice No. R. 225 of 2005 published under Government Gazette No. 27388 of 15 March 2005, as amended

intermediaries, any bribe, consideration, gift, reward, favour, or any material or immaterial benefit or any other advantage from the bidder, either for themselves or for any person, organisation or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

8.1.3 The GPG further confirms that its officials have not favoured any prospective bidder in any form that could afford an undue advantage to that bidder during the tendering stage and will further treat all bidders alike.

8.1.4 The GPG will during the tender process treat all Bidder(s) with equity.

8.1.5 All officials of the GPG shall report any attempted or completed violation of clauses to the following details:

	Gauteng Ethics Hotline	National Anti-Corruption Hotline
Toll-free number	080 1111 633	0800 701 701
SMS call-back	49017	N/A
E-mail	gpethics@behonest.co.za	nach@psc.gov.za
Fax	086 726 1681	0800 204 965
Website	www.thehotline.co.za	www.publicservicecorruptionhotline.org.za
Post	Chief Directorate: Integrity Management Private Bag X61 Marshalltown 2001	Public Service Commission Private X121 Pretoria 0001
Walk-in	Office of the Premier 55 Marshall Street Marshalltown Johannesburg 2001	Gauteng Provincial Office Public Service Commission Schreiner Chambers 6th Floor 94 Pritchard Street Johannesburg

8.1.6 Following the report on the violation of the above clauses by the official(s), through any source, the GPG shall investigate allegations of such violations against the official or other role players and when justified:

a) Take steps against such official and other role players (necessary disciplinary proceedings, and/or any other action as deemed fit, bar such officials from further dealings related to the contract process). In such a case, while an enquiry is being conducted by the Gauteng Provincial Government the proceedings under the contract would not be stalled.
b) Inform the relevant Treasury of steps taken in 8.1.5(a) against such officials; and
c) Report any conduct by such official and other role players that may constitute an offence to the South African Police Service.

9. COMMITMENTS OF THE BIDDERS

The bidder commits himself/herself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of his/her bid or during any pre-contract or post contract stage to secure the contract or in furtherance to secure it and commits himself/herself to the following:

9.1 The bidder is committed to doing business with integrity and proper regard for ethical business practices.

9.2 The bidder will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducements to any official of the Gauteng Provincial Government, connected directly or indirectly with the bidding process, or to any person, organisation or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

9.3 The bidder further undertakes that he/she has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducements to an official of the Gauteng Provincial Government or otherwise in procuring the contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Gauteng Provincial Government for showing or forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Gauteng Provincial Government.

9.4 The bidder will not collude with other parties interested in the contract to preclude the competitive bid price, impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

9.5 The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

9.6 The Bidder(s)/Contractor(s) will, when presenting his / her bid, disclose any and all payments he /she has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

9.7 In case of sub–contracting, the Principal Contractor shall take the responsibility of adoption of Integrity Pact by the Sub-Contractor.

9.8 The bidder shall report any attempted or completed violation of clauses 9.1 to 9.7 including any alleged unethical conduct to the Gauteng Ethics Hotline (details are provided at clause 8.1.4).

9.9 The bidder (or anyone acting on its behalf) warrants that:

9.9.1 It has not been convicted by a court of law for fraud and/or corruption with respect to the procurement/tendering processes; and/or

9.9.2 It has not been convicted by a court of law for theft or extortion; and/or

9.9.3 It is not listed on the National Treasury's database of Restricted Suppliers or Register of Tender Defaulters.

10. SANCTIONS FOR VIOLATION

10.1 The breach of any aforesaid provisions or providing false information by employers, including manipulation of information by evaluators, shall face administrative charges and penal actions as per the existing relevant rules and laws.

10.2 The breach of the Pact or providing false information by the Bidder, or anyone employed by him, or acting on his behalf (whether without the knowledge of the Bidder), or acting on his/her behalf, shall be dealt with as per the provisions of the Prevention and Combating of Corrupt Activities Act (12 of 2004).

10.3 The Gauteng Provincial Government shall also take all or any one of the following actions, wherever required:

10.3.1 To immediately call off the pre-contract negotiations without giving any compensation to the bidder. However, the proceedings with the other bidder(s) would continue.
10.3.2 To immediately cancel the contract, if already awarded/signed, without giving any compensation to the bidder.
10.3.3 To recover all sums already paid by the Gauteng Provincial Government.
10.3.4 To cancel all or any other contracts with the bidders and GPG shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value.
10.3.5 To submit the details of the bidder to the National Treasury to register on the database for tender defaulters.

11 CONFLICT OF INTEREST

11.1 A conflict of interest involves a conflict between the public duty and private interest (for favor or vengeance) of a public official, in which the public official has private interest which could improperly influence the performance of their official duties and responsibilities. Conflicts of interest would arise in a situation when any concerned members of both parties are related either directly or indirectly or has any association or had any confrontation. Thus, conflict of interest of any tender committee must be declared in a prescribed form.

11.2 The bidder shall not lend or borrow any money from or enter any monetary dealings or transactions, directly or indirectly, with any member of the tender committee or officials of the Gauteng Provincial Government, and if he/she does so, the Gauteng Provincial Government shall be entitled forthwith to rescind the contract and all other contracts with the bidder.

12 LEGAL ACTIONS

12.1 The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

13 VALIDITY

13.1 The validity of this Integrity Pact shall cover the tender process and extend until the completion of the contract to the satisfaction of both the Gauteng Provincial Government and the bidder (service provider).

13.2 Should one or several provisions of the Pact turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

GPG INTEGRITY PACT FOR BUSINESSES

BIDDER/SUPPLIER/SERVICE PROVIDER	
Signature of the CEO	
Full name of the CEO	
Tender number	
Date	

Annexure A

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

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

7.1 Within thirty (30) days of receipt of the notification of contract award,

security

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.