CITY OF CAPE TOWN
ISIXEKO SASEKAPA
STAD KAAPSTAD

Making progress possible. Together.

MEMORANDUM OF AGREEMENT

MADE AND ENTERED INTO BETWEEN

CITY OF CAPE TOWN METROPOLITAN MUNICIPALITY

And

BUSINESS CONNEXION (PTY) LTD

(REGISTRATION NO. [redacted])

[redacted]

PREAMBLE

WHEREAS Tender 265S/2019/20 was awarded to [redacted] ("Supplier" or "[redacted] on 15 February 2021 in line with resolution SCMB 53/02/21, for the Supply, Support, Maintenance and Services of ICT Security related infrastructure, software, services and licensing for the City of Cape Town for a period commencing from the commencement date enduring until 30 June 2025 ("the Tender").

AND WHEREAS in line with resolution SCMB 53/02/21, the conclusion of this Memorandum of Agreement between the City of Cape Town and the Supplier is subject to the conclusion of the process prescribed by section 33 of the Local Government: Municipal Finance Management Act 56 of 2003;

AND WHEREAS it is recorded that this Contract will be governed by the provisions of the Special Conditions of Contract, referring to the National Treasury – General Conditions of Contract (revised July 2010) ("**GCC**"), read with the Contract Specific Data ("**SCC**") as set out in the Contract.

NOW THEREFORE THE PARTIES AGREE AS FOLLOWS:

1. PARTIES

The Parties to this Contract are:

1.1. **The City of Cape Town**, a metropolitan municipality, established in terms of the Local Government: Municipal Structures Act. 117 of 1998 read with the Province of the Western Cape: Provincial Gazette 5588 dated 22 September 2000, as amended ("**the Purchaser or the City and used interchangeably**"), herein represented by the **City Manager or his nominee** and duly authorised hereto;

1.1.1. [redacted], a private company registered in terms of the laws of the Republic of South Africa with registration no [redacted] (the "**Supplier**" or "[redacted]"), herein represented by its duly authorised representative, [redacted] in his capacity as [redacted]

Executive: Coastal (Western Region); each a "**Party**" and together the "**Parties**".

2. INTERPRETATION AND DEFINITIONS

2.1 The headings in this MOA are inserted for reference purpose only and shall in no way govern or effect the interpretation of this MOA nor modify or amplify the terms of this MOA or any clause hereof.

2.2 Unless the context otherwise requires, reference to the singular shall include a reference to the plural, and vice versa, reference to any gender shall a reference to all other genders, and vice versa, and words importing natural persons shall include legal persons, and vice versa.

2.3 Any reference to "the Parties" or "a Party" will mean a reference to the City, the Supplier or both, depending on the context.

2.4 All annexures to this MOA form an integral part hereof and expressions defined in the MOA shall, unless the context otherwise requires, bear the same meaning in such annexures.

2.5 In the event of any conflict between the provisions of this Contract, the GCC and any Annexure attached hereto, or any other document incorporated by reference to this Contract, save to the extent expressly stated to the contrary, such conflict will be resolved by giving precedence to such different parts of this Contract in the following order of precedence:

2.5.1 first, the terms and conditions of the SCC;

2.5.2 second, the terms and conditions of the GCC;

2.5.3 third, Annexures and schedules to this Contract; and

[redacted]

2.5.4 fourth, any other documents incorporated by reference.

2.6 The provisions of this Contract supersede and replace the provisions of any previous agreement entered into between the Parties relating to the same subject matter.

2.7 Unless inconsistent with the context, the expressions set forth in this MOA shall bear the following meanings:

2.7.1	**"MOA"**	means this Memorandum of Agreement entered into between the City and the Supplier and shall supersede all agreements previously entered into;
2.7.2	**"the parties"**	means the Parties to this Agreement referred to in clause 1 and "**Party**" shall mean either of them;
2.7.3.	**"the tender"**	Means tender number 265S/2019/20 for the Supply, Support, Maintenance and Services of ICT Security related infrastructure, software, services and licensing for the City of Cape Town;
2.7.4.	**"the Commencement Date"**	Means the signature date;
2.7.5.	**"the completion date'**	Means 30 June 2025; and
2.7.6.	"**Signature Date**"	means the date on which this Agreement is signed by the Party signing last in time.

3 CONTRACT PERIOD

3.1 The Parties agree and record herein that the contract period for the MOA shall commence on the commencement date and terminate on the completion date.

[redacted]

3.2 Unless terminated earlier in accordance with the provisions as set out in the GCC or any other provision in terms of this Contract, this Contract shall commence on the commencement date and will terminate on 30 June 2025.

4 MUTUAL GOOD FAITH / CO-OPERATION

4.1 The Parties represent and undertake to do all such things, perform all such acts and take all steps to procure the doing of all such things and the performance of all such acts, as may be necessary or incidental to give effect to the execution of this Contract.

4.2 The Parties shall at all times during the continuance of this Contract observe the principles of good faith towards one another in the performance of their obligations in terms of this Contract.

5 OBLIGATIONS OF THE PURCHASER

5.1 The Purchaser undertakes to perform its obligations in accordance with the Contract, including but not limited to, the provision of the Goods and the supply of Services as set out in the conditions and specifications of the Tender, and subject to the satisfactory fulfilment of the obligations by the Supplier as set out in this Contract.

5.2 The Purchaser shall monitor and evaluate the Supplier's performance in respect of and in accordance with the provisions of this Contract, the GCC and any annexure and/or appendix attached hereto, or any other document incorporated by reference to this Contract, including the specifications and conditions of tender for the Tender.

6 OBLIGATIONS OF THE SUPPLIER

6.1 The Supplier hereby agrees and undertakes to provide the Goods and Supply the Services to the Purchaser as set out in this Contract, the GCC and any annexure and/or appendix attached hereto, or any other document incorporated by

reference to this Contract, including the specifications and conditions of tender for the Tender.

6.2 The Supplier will perform its obligations as expeditiously as possible and furthermore agrees and undertakes to provide the Goods and supply the Services in accordance with the operational requirements of the Purchaser.

6.3 The Supplier will ensure that the Goods provided and the Services supplied will be of a satisfactory quality and fit for purpose.

6.4 The Supplier shall, ensure that its employees, agents, representatives, subcontractors and suppliers comply with this Contract and all applicable Laws in the execution of its obligations to provide the Goods and supply the Services.

6.5 The Supplier will not conduct any activity of whatsoever nature which may be detrimental to the Purchaser's reputation and goodwill.

6.6 The Supplier undertakes to and in favour of the Purchaser that it – 6.6.1 has the resources, necessary expertise and skill, capabilities and technology to provide the Goods and supply the Services; and has effective, efficient and transparent financial management and control systems in place.

7 PRICING SCHEDULE

7.1 The Pricing Schedule for the provision of Goods and supply of Services shall be as set out in this MOA under Appendix A5 below.

7.2 The Supplier shall not be entitled to any other consideration for the provision of Goods and supply of Services other than as provided for in this Contract, the GCC and any annexure and/or appendix hereto, or any other document incorporated by reference to this Contract, including the specifications and conditions of tender for the Tender.

[redacted]

8 ENTIRE AGREEMENT

8.1 This Agreement constitutes the entire agreement between the Parties and no amendment, alteration, addition or variation of any right, term or condition of this Agreement will be of any force or effect unless reduced to writing and signed by the Parties to this Agreement.

8.2 The Parties agree that there are no conditions, variations or representations, whether oral or written and whether expressed or implied or otherwise, other than those contained in this Agreement.

8.3 This Agreement replaces any other previous verbal or written agreements entered into between the Parties.

8.4 The Conditions of Tender, returnable schedules and annexures which are required for tender evaluation purposes, shall form part of the contract arising from the invitation to tender. Accordingly, the conditions of tender and relevant returnable schedules, although not attached to this Contract, are specifically incorporated by way of reference and shall form part of the Contract between the parties.

9 WHOLE AGREEMENT, WAIVER AND VARIATION

9.1 This MOA embodies the whole agreement between the Parties. No other agreement, whether oral, implied or otherwise, will be of any force and effect unless it is reduced to writing and signed by the Supplier and the City, or their duly appointed representatives. There has been no representation which forms part of this MOA which has not been included herein.

9.2 Any relaxation, indulgence or waiver which the City may grant to the Supplier or any condonation by the City of any breach of the terms of this MOA will not become binding on the City. The City will at all times be entitled to claim due and prompt performance by the Supplier of all of the Suppliers' obligations in terms of this MOA.

9.3 No variation of the terms of this MOA will be of any force or effect unless reduced to writing and signed by the Supplier and the City, or their duly appointed representatives.

9.4 The Conditions of Tender, returnable schedules and annexures which are required for tender evaluation purposes, shall form part of the contract arising from the invitation to tender. Accordingly, the conditions of tender and relevant returnable schedules, although not attached to this Contract, are specifically incorporated by way of reference and shall form part of the Contract between the parties.

THE CITY OF CAPE TOWN:

Signature: [redacted]

Name:

Capacity:

Date:

Witness 1: [redacted]

Witness 2: [redacted]

SUPPLIER:

Signature: [redacted]

Name:

Capacity:

Date:

Witness 1: [redacted] Date: 12/8/2021

Witness 2: Date: 12/8/2021

[redacted]

APPENDIXES

A1	Form of Offer and Acceptance
A2	Special Conditions of Contract
A3	General Conditions of Contract
A4	Supporting Schedules
A5	Service Level Agreement
A6	Pricing Schedule
A7	Specifications

A1 – FORM OF OFFER AND ACCEPTANCE

(3) FORM OF OFFER AND ACCEPTANCE

TENDER 2659/2019/2020: SUPPLY, SUPPORT, MAINTENANCE OF ICT SECURITY RELATED INFRASTRUCTURE, SOFTWARE, SERVICES AND LICENSING

PART A (TO BE FILLED IN BY TENDERER):

2.1 Required Details (Please provide *applicable details* in full):

Name of Tendering Entity* ("the tenderer")	[redacted]
Trading as (if different from above)	

AND WHO IS represented herein by: (full names of signatory)
[redacted]

duly authorised to act on behalf of the tenderer in his capacity as: (title/ designation)
[redacted]

HEREBY AGREES THAT by signing the *Form of Offer and Acceptance*, the tenderer:

1. confirms that it has examined the documents listed in the Index (including Schedules and Annexures) and has accepted all the Conditions of Tender;
2. confirms that it has received and incorporated any and all notices issued to tenderers issued by the CCT;
3. confirms that it has satisfied itself as to the correctness and validity of the tender offer; that the price(s) and rate(s) offered cover all the goods and/or services specified in the tender documents; that the price(s) and rate(s) cover all its obligations and accepts that any mistakes regarding price(s), rate(s) and calculations will be at its own risk;
4. offers to supply all or any of the goods and/or render all or any of the services described in the tender document to the CCT in accordance with the:
   4.1 terms and conditions stipulated in this tender document;
   4.2 specifications stipulated in this tender document; and
   4.3 at the prices as set out in the Price Schedule (**Section 4**).
5. accepts full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on him in terms of the Contract.

[redacted]
Signature(s)

[redacted]
Print name(s):
On behalf of the tenderer (duly authorised)

16/3/2020
Date

[redacted]

[redacted]

PART B (TO BE FILLED IN BY THE CITY OF CAPE TOWN)

By signing this *Form of Offer and Acceptance* the City of Cape Town (also referred to as the 'Purchaser'):

1. accepts the offer submitted by ([redacted] **ALSO REFERRED TO AS THE "SUPPLIER")** _____, thereby concluding a contract with the supplier for a contract period commencing from date of commencement of contract and terminating 30 June 2025;

2. undertakes to make payment for the goods/services delivered in accordance with the terms and conditions of the Contract.

SIGNED AT_____ON THIS THE_____DAY OF_____20_____

(PLACE) (DD) (MM) (YY)

[redacted]

_____

Signature(s) and stamp of

Executive Director or his/ her delegated authority

_____

Print name(s):

(duly authorised in terms of the System

of Delegations as approved by Council)

[redacted]

FORM OF OFFER AND ACCEPTANCE (continued)

(TO BE FILLED IN BY THE CITY OF CAPE TOWN)

Schedule of Deviations

Notes:

1. The extent of deviations from the tender documents issued by the CCT before the tender closing date is limited to those permitted in terms of the conditions of tender.
2. A tenderer's covering letter shall not be included in the final contract document. Should any matter in such letter, which constitutes a deviation as aforesaid, become the subject of agreements reached during the process of offer and acceptance, the outcome of such agreement shall be recorded here.
3. Any other matter arising from the process of offer and acceptance either as a confirmation, clarification or change to the tender documents and which it is agreed by the Parties becomes an obligation of the contract shall also be recorded here.
4. Any change or addition to the tender documents arising from the above agreements and recorded here, shall also be incorporated into the final draft of the Contract.

1 Subject .....

Details .....

.....

.....

.....

2 Subject .....

Details .....

.....

.....

3 Subject .....

Details .....

.....

.....

.....

4 Subject .....

Details .....

.....

.....

.....

By the duly authorised representatives signing this agreement, the CCT and the tenderer agree to and accept the foregoing schedule of deviations as the only deviations from and amendments to this tender document and addenda thereto as listed in the returnable schedules, as well as any confirmation, clarification or changes to the terms of the offer agreed by the tenderer and the CCT during this process of offer and acceptance.

It is expressly agreed that no other matter whether in writing, oral communication or implied during the period between the issue of the tender documents and the receipt by the tenderer of a completed signed copy of this Agreement shall have any meaning or effect in the contract between the parties arising from this agreement.

A2 – SPECIAL CONDITIONS OF CONTRACT

The following Special Conditions of Contract, referring to the National Treasury – Conditions of Contract (revised July 2010), are applicable to this Contract:

1. Definitions

Delete Clause 1.15 and substitute with the following

1.15 The word 'Goods' is to be replaced everywhere it occurs in the GCC with the phrase 'Goods and / or Services' which means all of the equipment, machinery, materials, services, products, consumables, etc. that the supplier is required to deliver to the purchaser under the contract. This definition shall also be applicable, as the context requires, anywhere where the words "supplies" and "services" occurs in the GCC.

Delete Clause 1.19 and substitute with the following

1.19 The word 'Order' is to be replaced everywhere it occurs in the GCC with the words 'Purchase Order' which means the official purchase order authorised and released on the purchaser's SAP System and the date of the Purchase Order will be the contract commencement date

Delete Clause 1.21 and substitute with the following:

1.21 'Purchaser' means the [redacted] The address of the Purchaser is [redacted]

Add the following after Clause 1.25:

1.26 'Supplier' means any provider of goods and / or services with whom the contract is concluded

3. General Obligations

Delete Clause 3.2 in its entirety and replace with the following clauses.

3.2 The parties will be liable to each other arising out of or in connection with any breach of the obligations detailed or implied in this contract, subject to clause 28.

3.3 All parties in a joint venture or consortium shall be jointly and severally liable to the purchaser in terms of this contract and shall carry individually the minimum levels of insurance stated in the contract, if any.

[redacted]

3.4 The parties shall comply with all laws, regulations and bylaws of local or other authorities having jurisdiction regarding the delivery of the goods and give all notices and pay all charges required by such authorities.

3.5 The **supplier** shall:

3.5.1 Arrange for the documents listed below to be provided to the Purchaser prior to the issuing of the order:

a) Proof of Insurance (Refer to Clause 11) or Insurance Broker's Warrantee
b) Letter of good standing from the Compensation Commissioner, or a licensed compensation insurer (Refer to Clause 11)
c) Initial delivery programme
d) Other requirements as detailed in the tender documents

3.5.2 Only when notified of the acceptance of the bid by the issuing of the order, the supplier shall commence with and carry out the delivery of the goods in accordance with the contract, to the satisfaction, of the purchaser

3.5.3 Provide all of the necessary materials, labour, plant and equipment required for the delivery of the goods including any temporary services that may be required

3.5.4 Insure his workmen and employees against death or injury arising out of the delivery of the goods

3.5.5 Be continuously represented during the delivery of the goods by a competent representative duly authorised to execute instructions;

3.5.6 In the event of a loss resulting in a claim against the insurance policies stated in clause 11, pay the first amount (excess) as required by the insurance policy

3.5.7 Comply with all written instructions from the purchaser subject to clause 18

3.5.8 Complete and deliver the goods within the period stated in clause 10, or any extensions thereof in terms of clause 21

3.5.9 Make good at his own expense all incomplete and defective goods during the warranty period

3.5.10 Pay to the purchaser any penalty for delay as due on demand by the purchaser. The supplier hereby consents to such amounts being deducted from any payment to the supplier.

3.5.11 Comply with the provisions of the OHAS Act & all relevant regulations.

3.5.12 Comply with all laws relating to wages and conditions generally governing the employment of labour in the Cape Town area and any applicable Bargaining Council agreements.

3.5.13 Deliver the goods in accordance with the contract and with all reasonable care, diligence and skill in accordance with generally accepted professional techniques and standards.

3.6 The **purchaser** shall:

3.6.1 Issue orders for the goods required under this Contract. No liability for payment will ensue for any work done if an official purchase order has not been issued to the supplier.

3.6.2 Make payment to the **supplier** for the goods as set out herein.

3.6.3 Take possession of the goods upon delivery by the supplier.

3.6.4 Regularly inspect the goods to establish that it is being delivered in compliance with the contract.

3.6.5 Give any instructions and/or explanations and/or variations to the supplier including any relevant advice to assist the supplier to understand the contract documents.

3.6.6 Grant or refuse any extension of time requested by the supplier to the period stated in clause 10.

3.6.7 Inspect the goods to determine if, in the opinion of the purchaser, it has been delivered in compliance with the contract, alternatively in such a state that it can be properly used for the purpose for which it was intended.

3.6.8 Brief the supplier and issue all documents, information, etc. in accordance with the contract.

5. Use of contract documents and information; inspection, copyright, confidentiality, etc.

Add the following after clause 5.4:

5.5 Copyright of all documents prepared by the supplier in accordance with the relevant provisions of the copyright Act (Act 98 of 1978) relating to contract shall be vested in the purchaser. Where copyright is vested in the supplier, the purchaser shall be entitled to use the documents or copy them only for the purposes for which they are intended in regard to the contract and need not obtain the supplier's permission to copy for such use. Where copyright is vested in the purchaser, the supplier shall not be liable in any way for the use of any of the information other than as originally intended for the contract and the purchaser hereby indemnifies the supplier against any claim which may be made against him by any party arising from the use of such documentation for other purposes.

The ownership of data and factual information collected by the supplier and paid for by the purchaser shall, after payment, vest with the purchaser

5.6 Publicity and publication
The supplier shall not release public or media statements or publish material related to the services or contract within two (2) years of completion of the services without the written approval of the purchaser, which approval shall not be unreasonably withheld.

5.7 Confidentiality
Both parties shall keep all information obtained by them in the context of the Contract confidential and shall not divulge it without the written approval of the other party.

7. Performance Security

Delete clause 7.1 to 7.4 and replace with the following:

Not Applicable. Tenderers must disregard **Form of Guarantee / Performance Security** and are not required to complete same.

8. Inspections, tests and analyses

Delete Clause 8.2 and substitute with the following:

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 purchaser or an organisation acting on behalf of the purchaser.

10. Delivery and documents

Delete clauses 10.1 and 10.2 and replace with the following:

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The time for delivery of the goods shall be the date as stated on the order.

10.2 The purchaser shall determine, in its sole discretion, whether the goods have been delivered in compliance with the contract, alternatively in such a state that it can be properly used for the purpose for which it was intended. When the purchaser determines that the goods have been satisfactorily delivered, the purchaser must issue an appropriate certification, or written approval, to that effect. Invoicing may only occur, and must be dated, on or after the date of acceptance of the goods.

11. Insurance

Add the following after clause 11.1:

11.2 Without limiting the obligations of the supplier in terms of this contract, the supplier shall effect and maintain the following additional insurances:

a) Public liability insurances, in the name of the supplier, covering the supplier and the purchaser against liability for the death of or injury to any person, or loss of or damage to any property, arising out of or in the course of this Contract, in an amount not less than **R20 million** for any single claim;

b) Motor Vehicle Liability Insurance, in respect of all vehicles owned and / or leased by the supplier, comprising (as a minimum) "Balance of Third Party" Risks including Passenger Liability Indemnity;

c) Registration / insurance in terms of the Compensation for Occupational Injuries and Disease Act, Act 130 of 1993. This can either take the form of a certified copy of a valid Letter of Good Standing issued by the Compensation Commissioner, or proof of insurance with a licenced compensation insurer, from either the bidder's broker or the insurance company itself (see **Proof of Insurance / Insurance Broker's Warranty** section in document for a pro forma version).

d) Professional indemnity insurance providing cover in an amount of not less than R5 million in respect of each and every claim during the contract period

In the event of under insurance or the insurer's repudiation of any claim for whatever reason, the CCT will retain its right of recourse against the supplier.

11.3 The supplier shall be obliged to furnish the CCT with proof of such insurance as the CCT may require from time to time for the duration of this Contract. Evidence that the insurances have been effected in terms of this clause, shall be either in the form of an insurance broker's warranty worded precisely as per the pro forma version contained in the **Proof of Insurance / Insurance Broker's Warranty** section of the document or copies of the insurance policies.

15. Warranty

Add to Clause 15.2:

15.2 This warranty for this contract shall remain valid for **six (6) months** after the goods have been delivered.

16. Payment

Delete Clause 16.1 in its entirety and replace with the following:

16.1 A monthly payment cycle will be the norm. All invoices which are dated on or before the 20th of a particular month will typically be paid between the 23rd and 26th of the following month. The supplier may submit a fully motivated application regarding more frequent payment to the Employer for consideration. Requests for more frequent payments will be considered at the sole discretion of the Employer and is not a right in terms of this contract.

Delete Clause 16.2 in its entirety and replace with the following:

16.2 The supplier shall furnish the purchaser's Accounts Payable Department with an original tax invoice, clearly showing the amount due in respect of each and every claim for payment.

Add the following after clause 16.4

16.5 Notwithstanding any amount stated on the order, the supplier shall only be entitled to payment for goods actually delivered in terms of the Project Specification and Drawings, or any variations in accordance with clause 18. Any contingency sum included shall be for the sole use, and at the discretion, of the purchaser.

The CCT is not liable for payment of any invoice that pre-dates the date of delivery of the goods.

16.6 The purchaser will only make advanced payments to the supplier in strict compliance with the terms and details as contained on **Proforma Advanced Payment Guarantee**

17. Prices

Add the following after clause 17.1

17.2 The prices for the goods delivered and services performed shall not be subject to contract price adjustment

18. Contract Amendments

Delete the heading of clause 18 and replace with the following:

18. Contract Amendments and Variations

Add the following to clause 18.1:

Variations means changes to the goods or any extension of the duration of the contract that the purchaser issues to the supplier as instructions in writing, subject to prior approval by the purchaser's delegated authority as reflected on an authorised amended order. Should the supplier deliver any goods not described in a written instruction from the purchaser, such work will not become due and payable until amended order has been issued by the purchaser.

21. Delays in the supplier's performance

Delete Clause 21.2 in its entirety and replace with the following:

21.2 If at any time during the performance of the contract the supplier or its subcontractors should encounter conditions beyond their reasonable control which impede the timely delivery of the goods, the supplier shall notify the purchaser in writing, within 7 Days of first having become aware of these conditions, of the facts of the delay, its cause(s) and its probable duration. As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation, and may at his discretion extend the time for delivery.

Where additional time is granted, the purchaser shall also determine whether or not the supplier is entitled to payment for additional costs in respect thereof. The principle to be applied in this regard is that where the purchaser or any of its agents are responsible for the delay, reasonable costs shall be paid. In respect of delays that were beyond the reasonable control of both the supplier and the purchaser, additional time only (no costs) will be granted.

The purchaser shall notify the supplier in writing of his decision(s) in the above regard.

21.3 No provision in a contract shall be deemed to prohibit the obtaining of goods from a national department, provincial department, or a local authority.

22. Penalties

Delete clause 22.1 and replace with the following:

22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods 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 as stated herein for each day of the delay until actual delivery or performance.

The penalty for this contract shall be as per the Service Level Agreement.

23. Termination for default

Delete the heading of clause 23 and replace with the following:

23. Termination

Add the following to the end of clause 23.1:

if the supplier fails to remedy the breach in terms of such notice

Add the following after clause 23.7:

23.8 In addition to the grounds for termination due to default by the supplier, the contract may also be terminated:

23.8.1 Upon the death of the supplier who was a Sole Proprietor, or a sole member of a Close Corporation, in which case the contract will terminate forthwith.

23.8.2 The parties by mutual agreement terminate the contract.

23.8.3 If an Order has been issued incorrectly, or to the incorrect recipient, the resulting contract may be terminated by the purchaser by written notice

23.9 If the contract is terminated in terms of clause 23.8, all obligations that were due and enforceable prior to the date of the termination must be performed by the relevant party.

27. Settlement of Disputes

Amend clause 27.1 as follows:

27.1 If any dispute or difference of any kind whatsoever, with the exception of termination in terms of clause 23.1(c), arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve such dispute or difference amicably, by mutual consultation.

Delete Clause 27.2 in its entirety and replace with the following:

27.2 Should the parties fail to resolve any dispute by way of mutual consultation, either party shall be entitled to refer the matter for mediation before an independent and impartial person appointed by the City Manager in accordance with Regulation 50(1) of the Local Government: Municipal Finance Management Act, 56 of 2003 – Municipal Supply Chain Management Regulations (Notice 868 of 2005). Such referral shall be done by either party giving written notice to the other of its intention to commence with mediation. No mediation may be commenced unless such notice is given to the other party.

Irrespective whether the mediation resolves the dispute, the parties shall bear their own costs concerning the mediation and share the costs of the mediator and related costs equally.

The mediator shall agree the procedures, representation and dates for the mediation process with the parties. The mediator may meet the parties together or individually to enable a settlement.

Where the parties reach settlement of the dispute or any part thereof, the mediator shall record such agreement and on signing thereof by the parties the agreement shall be final and binding.

Save for reference to any portion of any settlement or decision which has been agreed to be final and binding on the parties, no reference shall be made by or on behalf of either party in any subsequent court proceedings, to any outcome of an amicable settlement by mutual consultation, or the fact that any particular evidence was given, or to any submission, statement or admission made in the course of amicable settlement by mutual consultation or mediation.

28. Limitation of Liability

Delete clause 28.1 (b) and replace with the following:

(b) the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the sums insured in terms of clause 11 in respect of insurable events, or where no such amounts are stated, to an amount equal to twice the contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

Add the following after clause 28.1:

28.2 Without detracting from, and in addition to, any of the other indemnities in this contract, the supplier shall be solely liable for and hereby indemnifies and holds harmless the purchaser against all claims, charges, damages, costs, actions, liability, demands and/or proceedings and expense in connection with:

a) personal injury or loss of life to any individual;
b) loss of or damage to property;

arising from, out of, or in connection with the performance by the supplier in terms of this Contract, save to the extent caused by the gross negligence or wilful misconduct of the purchaser.

28.3 The supplier and/or its employees, agents, concessionaires, suppliers, subcontractors or customers shall not have any claim of any nature against the purchaser for any loss, damage, injury or death which any of them may directly or indirectly suffer, whether or not such loss, damages, injury or death is caused through negligence of the purchaser or its agents or employees.

28.4 Notwithstanding anything to the contrary contained in this Contract, under no circumstances whatsoever, including as a result of its negligent (including grossly negligent) acts or omissions or those of its servants, agents or contractors or other persons for whom in law it may be liable, shall any party or its servants (in whose favour this constitutes a *stipulatio alteri*) be liable for any indirect, extrinsic, special, penal, punitive, exemplary or consequential loss or damage of any kind whatsoever, whether or not the loss was actually foreseen or reasonably foreseeable), sustained by the other party, its directors and/or servants, including but not limited to any loss of profits, loss of operation time, corruption or loss of information and/or loss of contracts.

28.5 Each party agrees to waive all claims against the other insofar as the aggregate of compensation which might otherwise be payable exceeds the aforesaid maximum amounts payable.

31. Notices

Delete clauses 31.1 and 31.2 and replace with the following:

31.1 Any notice, request, consent, approvals or other communications made between the Parties pursuant to the Contract shall be in writing and forwarded to the addresses specified in the contract and may be given as set out hereunder and shall be deemed to have been received when: a) hand delivered – on the working day of delivery

b) sent by registered mail – five (5) working days after mailing

c) sent by email or telefax – one (1) working day after transmission

32. Taxes and Duties

Delete the final sentence of 32.3 and replace with the following:

In this regard, it is the responsibility of the supplier to submit documentary evidence in the form of a valid Tax Clearance Certificate issued by SARS to the CCT at the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town ([redacted].

Add the following after clause 32.3:

32.4 The **VAT registration** number of the City of Cape Town is [redacted].

ADDITIONAL CONDITIONS OF CONTRACT

Add the following Clause after Clause 34:

35. Reporting Obligations.

35.1 The supplier shall complete, sign and submit with each delivery note, all the documents as required in the Specifications. Any failure in this regard may result in a delay in the processing of any payments.

36. Contract Period

36.1 It the intention of the City of Cape Town to run this tender subject to Section 33 of The Local Government Municipal Finance Management Act 56 of 2003 whereby this tender will impose financial obligations on the City for a period longer than the three

[redacted]

(3) financial years. The tender period is initially valid for the 3-years, thereafter the additional 2 years that is addressed in this tender document is subject to the City of Cape Town's Council approval via the Section 33 process.

A3 – GENERAL CONDITIONS OF CONTRACT

(National Treasury - General Conditions of Contract (revised July 2010))

TABLE OF CLAUSES

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

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 or her contractual obligations.

1.4 'Corrupt practice' means the offering, giving, receiving, or soliciting of anything 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 in which an enterprise abroad is subsidised 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 recognised 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 with 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 consignee's 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 markets its goods on its own initiative in the RSA at lower prices than that of the country of origin, and which action has the potential to harm the local industries in the RSA.

1.12 'Force majeure' means an event beyond the control of the supplier, not involving the supplier's fault or negligence, and not foreseeable. Such events

may include, but are 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 valueadding 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 organisation 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 the 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 the use of the goods or any part thereof by the purchaser.

7. Performance Security

7.1 Within 30 (thirty) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in the 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.

7.2 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 30 (thirty) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified in the 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 organisation acting on behalf of the Department.

8.3 If there are no inspection requirements indicated in the bidding documents and no mention of such 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 analysed 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 the 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 the 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 the SCC.

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

(a) performance or supervision of on-site assembly, and/or commissioning of the supplied goods;
(b) furnishing of tools required for the 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 the 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 12 (twelve) 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 18 (eighteen) 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 the SCC.

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

15.4 Upon receipt of such notice, the supplier shall, within the period specified in the 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 the 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 the SCC.

16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfilment of any other obligations stipulated in the contract.

16.3 Payments shall be made promptly by the purchaser, but in no case later than 30 (thirty) days after submission of an invoice or claim by the supplier.

16.4 Payment will be made in Rand unless otherwise stipulated in the 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 tendered by the supplier in his bid, with the exception of any price adjustments authorized in the 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 contract 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 the 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 or her 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 of supplies; or to have minor essential services executed if an emergency arises, or 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 cancelling 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 14 (fourteen) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated 14 (fourteen) 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 5 (five) 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, Act 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 of 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 antidumping or countervailing right is increased in respect of any dumped or subsidised 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 or she 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 or her.

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 notify the purchaser promptly, 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 such dispute or difference amicably, by mutual consultation.

27.2 If, after 30 (thirty) 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 to the supplier.

28. Limitation of Liability

28.1 Except in cases of criminal negligence or wilful 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 the 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, licence fees, and other such levies imposed outside the purchaser's country.

32.2 A local supplier shall be entirely responsible for all taxes, duties, licence 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, Act 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, Act 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 10 (ten) years and/or claim damages from the bidder(s) or contractor(s) concerned.

A4 – SUPPORTING SCHEDULES

tenderer schedule.

Schedule 2: Declaration for Procurement above R10 million

If the value of the transaction is expected to exceed R10 million (VAT included) the tenderer shall complete the following questionnaire, attach the necessary documents and sign this schedule:

1. Are you by law required to prepare annual financial statements for auditing? (Please mark with X)

YES	X	NO	

1.1 If YES, submit audited annual financial statements:

(I) for the past three years, or
(II) since the date of establishment of the tenderer (if established during the past three years)

By attaching such audited financial statements to List of other documents attached by tenderer schedule.

2. Do you have any outstanding undisputed commitments for municipal services towards the CCT or other municipality in respect of which payment is overdue for more than 30 (thirty) days? (Please mark with X)

YES		NO	X

2.1 If NO, this serves to certify that the tenderer has no undisputed commitments for municipal services towards any municipality for more than three (3) (three) months in respect of which payment is overdue for more than 30 (thirty) days.

2.2 If YES, provide particulars:

_____

_____

_____

_____

3. Has any contract been awarded to you by an organ of state during the past five (5) years? (Please mark with X)

YES	X	NO	

3.1 If YES, insert particulars in the table below including particulars of any material non-compliance or dispute concerning the execution of such contract. Alternatively attach the particulars to List of other documents attached by tenderer schedule in the same format as the table below:

Organ of State	Contract Description	Contract Period	Non-compliance/dispute (if any)
Health	Persal Support	36 months	N/A
Treasury	Persal Support	36 months	N/A
Treasury	KTSO (BI System)	24 months	N/A
DEDAT	App Development	36 months	N/A
Agriculture	SW Development 2	4 months	N/A

4. Will any portion of the goods or services be sourced from outside the Republic, and if so, what portion and whether any portion of payment from the CCT is expected to be transferred out of the Republic? (Please mark with X)

YES		NO	
			X

4.1 If YES, furnish particulars below

Please note that the products in Schedule H will be sourced from a local supplier but the pricing is subject to RoE fluctuations

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the employer of any other remedies available to it.

[redacted]

Signature

Print name

On behalf of the tenderer (duly authorised)

16/3/2020

Date

Schedule 4: Declaration of Interest – State Employees (MBD 4)

1. No bid will be accepted from persons in the service of the state*.

2. Any person, having a kinship with persons in the service of the state, including a blood relationship, may make an offer or offers in terms of this invitation to bid. In view of possible allegations of favouritism, should the resulting bid, or part thereof, be awarded to persons connected with or related to persons in service of the state, it is required that the tenderer or their authorised representative declare their position in relation to the evaluating/adjudicating authority.

3. In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.

3.1 Full Name of tenderer or his or her representative: [redacted]

3.2 Identity Number: [redacted]

3.3 Position occupied in the Company (director, trustee, shareholder²) [redacted] Region)

3.4 Company or Close Corporation Registration Number: [redacted]

3.5 Tax Reference Number: [redacted]

3.6 VAT Registration Number: [redacted]

3.7 The names of all directors / trustees / shareholders' members, their individual identity numbers and state employee numbers must be indicated in paragraph 4 below.

3.8 Are you presently in the service of the state? YES (NO)

3.8.1 If yes, furnish particulars .....

3.9 Have you been in the service of the state for the past twelve months? YES (NO)

3.9.1 If yes, furnish particulars .....

3.10 Do you have any relationship (family, friend, other) with persons in the service of the state and who may be involved with the evaluation and or adjudication of this bid? YES (NO)

3.10.1 If yes, furnish particulars .....

3.11 Are you, aware of any relationship (family, friend, other) between any other tenderer and any persons in the service of the state who may be involved with the evaluation and or adjudication of this bid? YES (NO)

3.11.1 If yes, furnish particulars .....

3.12 Are any of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state? YES (NO)

3.12.1 If yes, furnish particulars .....

3.13 Are any spouse, child or parent of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state? YES (NO)

3.13.1 If yes, furnish particulars .....

3.14 Do you or any of the directors, trustees, managers, principle shareholders, or stakeholders of

[redacted]

this company have any interest in any other related companies or business whether or not they are bidding for this contract? YES / NO

3.14.1 If yes, furnish particulars ..... Refer to CSD Report attached in Appendix C .....

4. Full details of directors / trustees / members / shareholders

Full Name	Identity Number	State Employee Number
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	N/A
[redacted]	[redacted]	N/A

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the employer of any other remedies available to it.

[redacted]

Signature Date 16/3/2020

Print name: [redacted]

On behalf of the tenderer (duly authorised)

'MSCM Regulations: "in the service of the state" means to be –

(a) a member of –
(i) any municipal council;
(ii) any provincial legislature; or
(iii) the national Assembly or the national Council of provinces;

(b) a member of the board of directors of any municipal entity;
(c) an official of any municipality or municipal entity;
(d) an employee of any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No.1 of 1999);
(e) an executive member of the accounting authority of any national or provincial public entity; or
(f) an employee of Parliament or a provincial legislature.

" Shareholder" means a person who owns shares in the company and is actively involved in the management of the company or business and exercises control over the company.

[redacted]

Schedule 5: Conflict of Interest Declaration

1. The tenderer shall declare whether it has any conflict of interest in the transaction for which the tender is submitted. (Please mark with X)

YES		NO	X

1.1 If yes, the tenderer is required to set out the particulars in the table below:

2. The tenderer shall declare whether it has directly or through a representative or intermediary promised, offered or granted:

2.1 any inducement or reward to the CCT for or in connection with the award of this contract; or

2.2 any reward, gift, favour or hospitality to any official or any other role player involved in the implementation of the supply chain management policy. (Please mark with X)

YES		NO	X

If yes, the tenderer is required to set out the particulars in the table below:

Should the tenderer be aware of any corrupt or fraudulent transactions relating to the procurement process of the City of Cape Town, please contact the following:

the City's anti-corruption hotline at [redacted] (toll free)

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the employer of any other remedies available to it.

[redacted]

Signature

Print name: Boedall Swarts

On behalf of the tenderer (duly authorised)

16/3/2020

Date

[redacted]

Schedule 9: Occupational Health and Safety Agreement

AGREEMENT MADE AND ENTERED INTO BETWEEN THE CITY OF CAPE TOWN (HEREINAFTER CALLED THE "CCT") AND

[redacted] ,
(Supplier/Mandatary/Company/CC Name)

IN TERMS OF SECTION 37(2) OF THE OCCUPATIONAL HEALTH AND SAFETY ACT, 85 OF 1993 AS AMENDED.

I, [redacted] , representing

[redacted] , as an employer

in its own right, do hereby undertake to ensure, as far as is reasonably practicable, that all work will be performed, and all equipment, machinery or plant used in such a manner as to comply with the provisions of the Occupational Health and Safety Act (OHSA) and the Regulations promulgated thereunder.

I furthermore confirm that I am/we are registered with the Compensation Commissioner and that all registration and assessment monies due to the Compensation Commissioner have been fully paid or that We are insured with an approved licensed compensation insurer.

COID ACT Registration Number: [redacted]

OR Compensation Insurer: ..... Policy No.: .....

I undertake to appoint, where required, suitable competent persons, in writing, in terms of the requirements of OHSA and the Regulations and to charge him/them with the duty of ensuring that the provisions of OHSA and Regulations as well as the Council's Special Conditions of Contract, Way Leave, Lock-Out and Work Permit Procedures are adhered to as far as reasonably practicable.

I further undertake to ensure that any subcontractors employed by me will enter into an occupational health and safety agreement separately, and that such subcontractors comply with the conditions set.

I hereby declare that I have read and understand the Occupational Health and Safety Specifications contained in this tender and undertake to comply therewith at all times.

I hereby also undertake to comply with the Occupational Health and Safety Specification and Plan submitted and approved in terms thereof.

Signed at Cape Town on the 16 day of March 20 20

[redacted]
Witness

[redacted]
Mandatary

Signed at ..... on the ..... day of ..... 20 ....

[redacted]
Witness

[redacted]
for and on behalf of
City of Cape Town

[redacted]

[redacted]

Schedule 10: Certificate of Independent Tender Determination

I, the undersigned, in submitting this tender
SUPPLY, SUPPORT, MAINTENANCE OF ICT SECURITY RELATED INFRASTRUCTURE, SOFTWARE, SERVICES AND LICENSING

In response to the tender invitation made by THE CITY OF CAPE TOWN, do hereby make the following statements, which I certify to be true and complete in every respect:

I certify, on behalf of: [redacted] (Name of tenderer)

That:

1. I have read and I understand the contents of this Certificate;
2. I understand that this tender will be disqualified if this Certificate is found not to be true and complete in every respect;
3. I am authorised by the tenderer to sign this Certificate, and to submit this tender, on behalf of the tenderer;
4. Each person whose signature appears on this tender has been authorised by the tenderer to determine the terms of, and to sign, the tender on behalf of the tenderer;
5. For the purposes of this Certificate and this tender, I understand that the word 'competitor' shall include any individual or organisation other than the tenderer, whether or not affiliated with the tenderer, who:
   (a) has been requested to submit a tender in response to this tender invitation;
   (b) could potentially submit a tender in response to this tender invitation, based on their qualifications, abilities or experience; and
   (c) provides the same goods and services as the tenderer and/or is in the same line of business as the tenderer.
6. The tenderer has arrived at this tender independently from and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium[1] will not be construed as collusive price quoting.
7. In particular, without limiting the generality of paragraphs 5 and 6 above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:
   (a) prices;
   (b) geographical area where product or service will be rendered (market allocation);
   (c) methods, factors or formulas used to calculate prices;
   (d) the intention or decision to submit or not to submit a tender;
   (e) the submission of a tender which does not meet the specifications and conditions of the tender; or
   (f) tendering with the intention not to win the contract.
8. In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications and conditions or delivery particulars of the products or services to which this tender invitation relates.
9. The terms of this tender have not been and will not be disclosed by the tenderer, directly or indirectly, to any competitor, prior to the date and time of the official tender opening or of the awarding of the contract.
10. I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to tenders and contracts, tenders 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, Act 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 10 (ten) years in terms of the Prevention and Combating of Corrupt Activities Act, Act 12 of 2004, or any other applicable legislation.

[redacted]
Signature

16/3/2020
Date

Friedall Swarts
Name (PRINT)
(For and on behalf of the Tenderer (duly authorised))

[redacted]

A5 – SERVICE LEVEL AGREEMENT

SUPPLY, SUPPORT, MAINTENANCE AND SERVICES OF

ICT SECURITY SERVICES`

these being

Reverse Proxy Services

Vulnerability Management Services

Citrix Virtual Desktop Infrastructure or equivalent

IT Security Intelligence Systems (managed by The City)

IT Security Intelligence Systems (managed by the Service Provider)

Data Loss Prevention Solutions

Anti-malware solutions & Email Hygiene

Security Assessment Services

Cloud Access Service Broker

Between

CITY OF CAPE TOWN

(of the one part)

and

[redacted] (Company)

(of the other part)

[redacted]

1. INTERPRETATION AND DEFINITIONS

1.1 In this Agreement and unless the context otherwise requires: -

1.1.1 words, including their definitions in clause 1.4, which import the singular number only, shall include the plural and vice versa;
1.1.2 words importing persons shall include bodies corporate;
1.1.3 words importing the singular, includes the plural and vice versa.

1.2 The head notes to the various clauses of this Agreement are inserted for reference purposes only and shall in no way govern or affect the construction hereof.

1.3 All references to this Service Level Agreement shall be references to this Agreement and all Annexures hereto, which Annexures form an integral part of this Agreement, and expressions defined in this Agreement shall bear the same meanings when used in any Annexure to this Agreement and vice versa.

1.4 Unless the context otherwise requires, the under-mentioned expressions shall have the meanings respectively assigned to them hereunder, namely: -

Access	right or opportunity to reach or visit (to gain access); security and keys;
Accessories	not part of basic equipment, additional or extra items;
Accident	unfortunate, usually harmful event, caused unintentionally Third Party Liability: _____(Company) must insure against eventuality (personal or equipment) at _____(Company)'s expense; comply with COIDA. Refer to Clause 11: Insurance under the General Conditions of Contract as contained on page 193 of the Tender Document and Special Conditions of Contract as contained on page 184 of the Tender Document;
Authorised Person	appointed and duly authorised respectively by representative the City and the Supplier, to act (and speak) upon the respective party's behalf;
"City"	City" means the City of Cape Town, a municipality established by the City of Cape Town Establishment Notice No. 479 of 22 September

	2000, issued in terms of the Local Government: Municipal Structures Act, 1998, (Act 117 of 1998) or any structure or employee of the City acting in terms of delegated authority;
"Commencement date of signature of last party hereto or date as agreed date" by both parties in this agreement – kicks in 30 days after going live, anticipated date is 1 JULY 2020;	
"Contract Management"	Monthly statistical reporting on service levels;
Defects	faults, imperfection in manufacture or shortcoming of equipment possibly causing other components to become faulty;
Equipment	Any associated material required for solution infrastructure;
Failure	1. breaking down or ceasing to function 2. non-performance of duties or responsibilities;
Guarantees	undertaking to answer and compensate for the loss of performance or for an obligation by another person. Refer to Clause 7 of the Special Conditions of Contract; Annexure 1: Form of Guarantee / Performance Security in the Tender Document;
Grief Point	Objective measure of a penalty to be applied in the event of a required performance metric not being met as defined by the City
Job Completion	To be considered complete, each job must be signed off by the line department before the City will entertain honoring an invoice.
Line departments	Departments within the organizational structure of the City.
Malfunction	When equipment fails to function normally;
Misuse	wrong or improper use or application of equipment;
Negligence	Lack of proper care and attention;
Normal working hours	Hours between 08:00 and 16:30 from Monday to Friday, excluding public holidays;
"Parties"	the City and the Supplier collectively;

Repairs	Restore to good, working condition after damage, wear or malfunction;
"Reporting"	Timely periodic reporting on monthly meetings in the format as agreed upon between City of Cape Town and _____(Company);
Resolution	System is repaired and made operationally available;
Response	Representative from _____(Company) arrives on-site or email acknowledgement that _____(Company) has received a request for work
Service agent	Authorised technician, able to perform to specified requirements
"Service Level"	the required quantitative level or degree of performance of the Services by the Supplier as set out by Service Level Measure, see the Service Level Measurements Section;
"Service Level Agreement ("SLA")"	the agreement concluded between the parties as evidenced in this written document, any annexures and the related tender;
"Service Level Measure"	the method specified in this Service Level Agreement for quantitatively calculating the Supplier's actual performance. The results of these calculations are compared with Service Levels to evaluate the Supplier's compliance with Service Levels, see the Service Level Measurements Section;
"Service Level Termination Event"	an event wherein the City shall have the option, but not the obligation, to terminate this agreement without further obligations;
"Service Penalty"	the amount calculated which the City shall have the option, but not the obligation, to recover as a reduction in the fee payable for the Services, each time the Supplier fails to meet the Service Levels, reference clause 22: Penalties of the Special Conditions of Contract

"Stock Management"	Stock levels of appropriate spares and equipment of the right quality and quantity in the right location to enable the Supplier to operate within the agreed upon for response;
Sundries	items or oddments not mentioned individually;
"Supplier"	_____(Company), Registration Number: _____ of physical address: _____; Postal address: _____, a company duly incorporated in accordance with the company laws of South Africa, represented herein by _____, who warrants that he/she is duly authorised by board resolution to sign this Agreement for and on behalf of the Supplier. The Supplier warrants that- 1. it is registered under the Regional Services Council Act, 1985, under registration number. CMC RSC Levy # _____, for the purpose of the payment of all levies payable by it under that Act; and 2. all levies due by it under such Act to date hereof, have been paid; "Supplier" is a generic term which may include suppliers of goods and services, contractors and/or consultants;
Technical skills	technical ability / expertise of installation and test equipment technicians
Useful life	Minimum duty cycle of equipment or components
Warranties	undertaking as to the ownership or quality of an item, accepting responsibility for defects or repairs over a specified period. Refer to Clause 15 of the General Conditions of Contract as contained on page 185 of the Tender document and Clause 15 of Special Conditions of Contract;
Working day	Any day between Monday and Friday, 08:00 till 17:00, excluding Saturdays, Sundays and Public Holidays

Working hours	Eight hours in any given working day

2 SERVICE LEVELS

2.1 These Service Levels are the minimally acceptable level of service as detailed hereunder for the Services and failure to comply may give rise to the calculation of Service Penalties and they may give rise to a Service Level Termination Event.

2.2 Any failure to meet a Service Level is unacceptable and may constitute a material breach of the Supplier's obligations.

2.3 Maximum Delivery Period - on-site within six weeks of purchase order date. Failure to comply may result in defaulting the preferred supplier and ultimately, suspension.

2.4 Communication Plan

E-mail is the preferred means of communication between the Supplier and the City of Cape Town.

The City's authorised representatives, see names below, will provide _____ (Company)'s authorised representatives, see names below, with an Order number by Fax or email. This number must be reflected on the related invoice. _____ (Company)'s must send an email acknowledgement within the following timeframes of receiving an order or request for a warranty repair or replacement:

When order received	08:00 to 17:00	After 17:01 and weekends
Response	Before 17:00 next business day	Before 17:00 next business day

_____ (Company)'s contact details:

Procurement or orders

Authorised Representative	Name: [redacted] Tel number: [redacted] Email add [redacted] Fax Num	Provide Percentage of not meeting Service Level (Example 60%) [redacted]
Escalation Level 1	Name: [redacted] Tel number: [redacted] Email add [redacted] Fax Num	Provide Percentage of not meeting Service Level (Example 80%) [redacted]
Escalation Level 2	Name: [redacted] Tel number: [redacted] Email add [redacted] Fax Num	

Warranty or fault Repairs / Replacement

Authorised Representative	Name: [redacted] Tel number: [redacted] Email add [redacted] Fax Num	Provide Percentage of not meeting Service Level (Example 60%) [redacted]

[redacted]

Escalation Level 1	Name: [redacted] Tel number [redacted] Email add [redacted] Fax Num_____	Provide Percentage of not meeting Service Level (Example 80%) [redacted]%
Escalation Level 2	Name: _____ Tel number:_____ Email add_____ Fax Num_____	

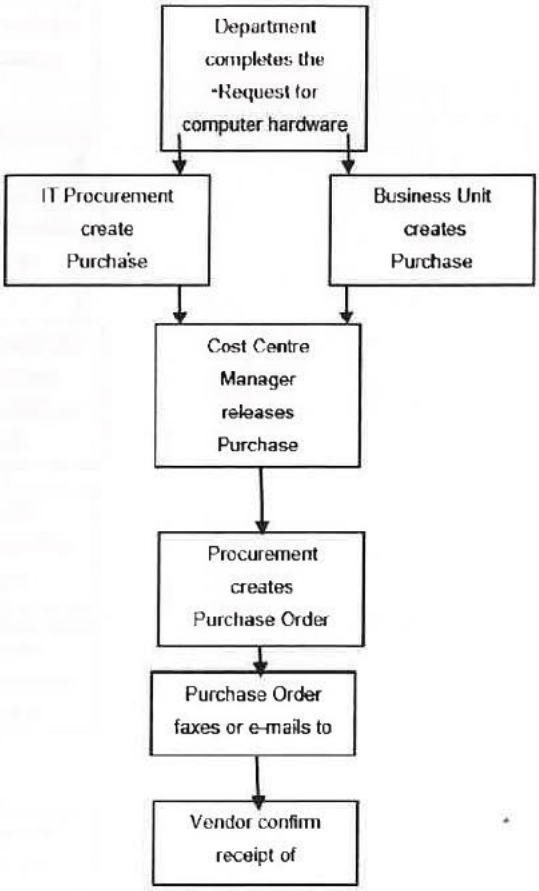
City of Cape Town contact detail:

Procurement

Authorised representative: [redacted]
E-Mail address: [redacted]
Telephone Number: [redacted]
Fax Number: [redacted]

City of Cape Town Procurement process:

[redacted]



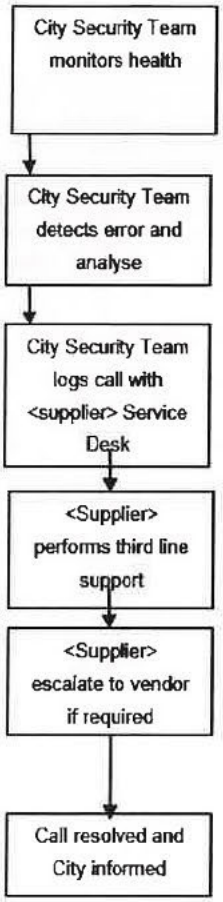
Warranty Repairs / Services / Fault Reporting

Authorised representative: [redacted]
E-mail address: [redacted]
Telephone number: [redacted]

[Insert your process flow to request warranty repairs or a service or to report a fault]

Insert process flow from above and modify – just log call

[redacted]


City Security Team monitors health
City Security Team detects error and analyse
City Security Team logs call with <supplier> Service Desk
<Supplier> performs third line support
<Supplier> escalate to vendor if required
Call resolved and City informed

2.5 Roles and Responsibilities

The Supplier

Party	Functional Role	Service Responsibility
Service Provider	Maintain guaranteed service levels and service assurance	Logging and tracking of contractual incidents for all problems from receipt of issue from City to resolution.
Service Provider	Performance Management Report	Quarterly reports to the City
Service Provider	Contractual Incident Report	Quarterly reports to the City
Service Provider	Supply and delivery of goods	Supply and deliver of equipment within a period of six weeks from date of purchase order received from City
Service Provider	SLA measurement	Calculation of any Service Credits if due
Service	Adherence to all change control,	Communication with City contacts only
Provider	maintenance and emergency procedures	
Service Provider	Support and maintenance	Provide support and maintenance services from receipt of logged call from City This includes managing escalation procedures to the vendor support centre
Service Provider	Solution Design	Drafting of solution designs, scenarios and associated quotations in order to meet the information security requirements of the City of Cape Town
City of Cape Town IS & T department	Request for solutions	Clearly defined requirements
City of Cape Town IS & T department	Generate purchase order	Supply orders with official City order number, delivery address and contact person
City of Cape Town IS & T department	Taking receipt of goods, and support and maintenance certificates	Sign Invoices or delivery notes on delivery of orders

City of Cape Town IS & T department	Fault notification	Log support calls with supplier with relevant details
City of Cape Town IS & T department	SLA measurement	Measure and /or audit the measurement of delivery schedule, arrange Goods Receipt Note (GRN)

Line departments other than IS&T

1. Request quotes from IS&T
2. Raise Purchase Requisition
3. Release Purchase Requisition on SAP
4. On delivery of ordered equipment, sign the Receipt or Delivery note
5. GRN the Purchase Order

2.6 Scope

2.6.1 In-Scope

- Quotations
- Solution design and proposals
- Supply and delivery of services, licenses, goods, and support and maintenance certificates
  Support and maintenance processes with supplier

2.6.2 Out-of-Scope

- Informal telephonic queries

2.7 Description of Services:

- Quotations
- Support and maintenance
- Log calls with vendor
- Management of vendor processes on behalf of the City

Types of equipment:

- Appliances - various
- Servers
- On premise

Refer to Pricing Schedules within the tender document, regarding the SLA costs to be provided in order to meet the terms and conditions of the Service Level Agreement measurements as per Schedules listed below.

3 SERVICE LEVEL MEASUREMENTS

3.1 The provision of each Service will be measured by comparing the level at which the actual Services are provided against the level at which the parties agreed that the Services will be provided as set out below;

3.2 The method that the parties will use to make this comparison is set out below:

3.1 Schedule A: Reverse Proxy

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
1.	Device Availability	Uptime of each individual Reverse Proxy Device	Not defined	–
2.	Service Availability	Uptime of the Reverse Proxy service	Not defined	–
3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than 60 minutes	5 Grief Points
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Remediate configuration issues within one (1) full Working Day	5 Grief Points
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Provided (yes / no) Assessed monthly by random check Note: non-availability of technical support may result in Device and/or Service Unavailability, and will be penalised consequently	5 Grief Points
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points

		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Design Proposals provides within ten (10) full Working Days (yes / no)	5 Grief Points
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	1 Grief Point
		Equipment Delivery process followed as specified	Specified items delivered – not defined	–
			Packaging as specified – not defined	–
			Labelling as specified – not defined	–
			Delivery within quoted lead time - not defined	–
			Delivery at the place specified in the Purchase Order – not defined	–
		Fault handling process followed	Not defined	–
		Repair or replacement process followed	Not defined	–
7.	Report to the City	Provide monthly Summary Report as specified, including record of all Incidents and related resolutions, plus	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points

		root cause when requested		
		Report on an outstanding software updates, security updates and related recommendations	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
8.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Present as per attendance register (yes/no) Assessed per meeting as evidenced by Attendance Register	2 Grief Points

3.2 Schedule B: Vulnerability Management (VM)

#	Service Element	Service Measure	Service Metric	Grief Points incurred for non-performance
1.	Device Availability	Uptime of each individual Device	Not defined	–
2.	Service Availability	Uptime of the Vulnerability Management service	Not defined	–
3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than eight (8) consecutive hours	5 Grief Points
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Remediate reconfiguration issues within three (3) full	5 Grief Points

			Working Days	
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Provided (yes / no) Assessed monthly by random check Note: non-availability of technical support may result in Device and/or Service Unavailability, and will be penalised consequently	5 Grief Points
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points
		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Design Proposals provides within ten (10) full Working Days (yes / no)	5 Grief Points
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	2 Grief Points
		Equipment Delivery process followed as	Specified items delivered – not defined	–
		specified	Packaging as specified – not defined	–
			Labelling as specified – not defined	–

			Delivery within quoted lead time - not defined	–
			Delivery at the place specified in the Purchase Order – not defined	–
		Fault handling process followed	As specified (yes / no)	3 Grief Points
		Repair or replacement process followed	As specified (yes / no)	3 Grief Points
7.	Report to the City	Provide monthly Summary Report as specified Include record of all Incidents and consequent resolutions, plus root cause when requested	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
		Report on an outstanding software updates, security updates and related recommendations	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
		Monthly report to include five assessments of vulnerability scans as per schedule, to be provided by the City, to ensure appropriate configuration using best practice	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	1 Grief Point
8.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Present as per attendance register (yes/no) Assessed per meeting as evidenced by	2 Grief Points

			Attendance Register	

3.3 Schedule C: Citrix Virtual Desktop Infrastructure or equivalent

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
1.	Device Availability (ref. clause 6.1)	Uptime of each individual VDI server	Not defined	–
2.	Service Availability (ref. clause 6.2)	Uptime of the VDI service	Not defined	–
3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than 60 minutes	5 Grief Points
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Remediate reconfiguration issues within three (3) full Working Days	5 Grief Points
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Provided (yes / no) Assessed monthly by random check Note: non-availability of technical support may result in Device and/or Service Unavailability, and will be penalised consequently	5 Grief Points

5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points
		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Design Proposals provides within ten (10) full Working Days (yes / no)	5 Grief Points
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	1 Grief Point
		Equipment Delivery process followed as	Specified items delivered – not defined	–
7.		specified	Packaging as specified – not defined	–
			Labelling as specified – not defined	–
			Delivery within quoted lead time - not defined	–
			Delivery at the place specified in the Purchase Order – not defined	–
		Fault handling process followed	Not defined	–
		Repair or replacement process followed	Not defined	–
8.	Report to the City	Provide monthly Summary Report as specified	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points

9.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points

3.4 Schedule D: IT Security Intelligence (managed by The City)

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
1.	Device Availability	Not applicable	Not defined	--
2.	Service Availability	Not applicable	Not defined	--
3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than four (4) hours	5 Grief Points
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Not defined	--
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Remediate configuration issues within three (3) full Working Days	5 Grief Points
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points
		Key Contact Person responds timeously	Not defined	--
6.	Adhere to procurement, ordering, delivery	Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	2 Grief Points

	and payment process	Equipment Delivery process followed as specified	Specified items delivered – not defined	--
			Packaging as specified – not defined	--
			Labelling as specified – not defined	--
			Delivery within quoted lead time – not defined	--
			Delivery at the place specified in the Purchase Order – not defined	--
		Fault handling	Not defined	--
7.		process followed		
		Repair or replacement process followed	Not defined	--
8.	Report to the City	Provide monthly Summary Report as specified Include record of all incidents and consequent resolutions, plus root cause when requested	Provided within seven (7) Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
		Include details of outstanding security updates, software updates, and any related recommendations		1 Grief Point

9.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Present as per attendance register (yes/no) Assessed per meeting as evidenced by Attendance Register	2 Grief Points

3.5 Schedule D: IT Security Intelligence (managed by the Service Provider)

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
1.	Device Availability	Uptime of each individual logging unit or appliance	Better than or equal to 99% over the period of each Calendar month	10 Grief Points
2.	Service Availability	Uptime of the IT Security Intelligence Platform	Better than or equal to 99.9% over the period of each Calendar month	15 Grief Points
3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than thirty (30) minutes	5 Grief Points
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Not defined	–
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Remediate configuration issues within three (3) full Working Days	5 Grief Points

[redacted]

		Train City staff on the functionality of the platform sufficient to ensure service continuity	Eight (8) full Working Hours per Calendar Month, as evidenced by signed job card	2 Grief Points
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points
		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Design Proposals provides within ten (10) full Working Days (yes / no)	2 Grief Points
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	1 Grief Point
		Equipment Delivery process followed as	Specified items delivered – not defined	–
7.		specified	Packaging as specified – not defined	–
			Labelling as specified – not defined	–
			Delivery within quoted lead time – not defined	–
			Delivery at the place specified in the Purchase Order – not defined	–
		Fault handling process followed	As specified – not defined	–
		Repair or replacement process followed	As specified – not defined	–

8.	Report to the City	Provide monthly Summary Report as specified Include record of all Incidents and consequent resolutions, plus root cause when requested	Provided within seven (7) Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
		Include details of outstanding security updates, software updates, and any related recommendations		1 Grief Point
9.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Present as per attendance register (yes/no) Assessed per meeting as evidenced by Attendance Register	2 Grief Points

3.6 Schedule E: Data Loss Prevention

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
1.	Device Availability	Uptime of Devices	Not defined	–
2.	Service Availability	Uptime of the Service	Not defined	–
3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than four (4) hours	5 Grief Points

[redacted]

		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Not defined	–
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Remediate configuration issues within three (3) full Working Days	5 Grief Points
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points
		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Design Proposals provides within ten full Working Days (yes / no)	5 Grief Points
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	1 Grief Point
		Equipment Delivery process followed as specified	Specified items delivered – not defined	–
			Packaging as specified (yes / no)	–
			Labelling as specified – not defined	–
			Delivery within quoted lead time – not defined	–
			Delivery at the place specified in the	–

			Purchase Order – not defined	
		Fault handling process followed	Not defined	–
		Repair or replacement process followed	Not defined	–
7.	Report to the City	Provide monthly Summary Report as specified Include record of all Incidents and consequent resolutions, plus root cause when requested	Provided within seven (7) Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
		Include details of outstanding security updates, software updates, and any related recommendations		1 Grief Point
8.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Present as per attendance register (yes/no) Assessed per meeting as evidenced by Attendance Register	2 Grief Points

3.7 Schedule F: Anti-malware solutions & Email Hygiene

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
1.	Device Availability	Uptime of Devices	Not defined	–
2.	Service Availability	Uptime of the Malware Protection service	Not defined	–

3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than two (2) hours	5 Grief Points
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Four (4) hours	10 Grief Points
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Remediate configuration issues within three (3) full Working Days	5 Grief Points
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points
		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Design Proposals provides within ten full Working Days (yes / no)	5 Grief Points
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	1 Grief Point
		Equipment Delivery process followed as specified	Specified items delivered – not defined	–
			Packaging as specified (yes / no)	–
			Labelling as specified – not defined	–
			Delivery within quoted lead time – not defined	–

			Delivery at the place specified in the Purchase Order – not defined	–
		Fault handling process followed	Not defined	–
		Repair or replacement process followed	Not defined	–
7.	Report to the City	Provide monthly Summary Report as specified Include record of all Incidents and consequent resolutions, plus root cause when requested	Provided within seven (7) Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
		Include details of outstanding security updates, software updates, and any related recommendations		1 Grief Point
8.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Present as per attendance register (yes/no) Assessed per meeting as evidenced by Attendance Register	2 Grief Points

3.8 Schedule G: Security assessment services

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
1.	Device Availability	Not applicable	Not defined	–

2.	Service Availability	Not applicable	Not defined	–
3.	Incident Response	Mean Time To Respond (MTTr) – attributed to a security risk assessment	Not defined	–
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Not defined	–
		Maximum Time To Replace ($TTRp^{MAX}$)	Not defined	–
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Not defined	–
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	–
		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Not defined	–
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	–
		Equipment Delivery process followed as specified	Specified items delivered – not defined	–
			Packaging as specified (yes / no) - not defined	–
			Labelling as specified – not defined	–

			Delivery within quoted lead time – not defined	–
			Delivery at the place specified in the Purchase Order – not	–
			defined	
		Fault handling process followed	Not defined	–
		Repair or replacement process followed	Not defined	–
7.	Report to the City	Provide monthly Summary Report as specified Include record of all incidents and consequent resolutions, plus root cause when requested	Not defined	–
		Include details of outstanding security updates, software updates, and any related recommendations		–
8.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Not defined	–

3.9 Schedule H: Cloud Access Service Broker (CASB)

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance

1.	Device Availability	Uptime of CASB devices	Not defined	–
2.	Service Availability	Uptime of the CASB service	Not defined	–
3.	Incident Response	Mean Time To Respond (MTTr) – Priority 1, 2 & 3 Incidents	Less than five (5) minutes	5 Grief Points
		Maximum Time To Restore (TTR^{MAX}) – Priority 1 & 2 Incidents	Not defined	–
		Maximum Time To Replace ($TTRp^{MAX}$)	Five (5) full Working Days	5 Grief Points
4.	Provide Maintenance and Technical Support	Technical support services available as specified	Remediate configuration issues within three (3) full Working Days	5 Grief Points
5.	Provide and maintain Contact Information	Provide and maintain contact details	Provided (yes/no) Assessed monthly by random check	2 Grief Points
		Key Contact Person responds timeously	Not defined	–
6.	Adhere to procurement, ordering, delivery and payment process	Responses to requests for Design Proposals as required	Design Proposals provides within ten (10) full Working Days (yes / no)	5 Grief Points
		Responses to requests for Quotations provided as required	Quotations provided within seven (7) full Working Days (yes / no)	1 Grief Point
		Equipment Delivery process followed as specified	Specified items delivered – not defined	–
			Packaging as specified (yes / no)	–

			Labelling as specified – not defined	–
			Delivery within quoted	–
7.			lead time – not defined	
			Delivery at the place specified in the Purchase Order – not defined	–
		Fault handling process followed	Not defined	–
		Repair or replacement process followed	Not defined	–
8.	Report to the City	Provide monthly Summary Report as specified Include record of all Incidents and consequent resolutions, plus root cause when requested	Provided within seven (7) Calendar Days after the last day of each month (yes/no) Assessed monthly	2 Grief Points
		Include details of outstanding security updates, software updates, and any related recommendations		1 Grief Point
8.	Attend Service Review Meetings	Physical attendance at the Service Review Meeting of the Key Contact Person	Present as per attendance register (yes/no) Assessed per meeting as evidenced by Attendance Register	2 Grief Points

4 FREQUENCY FOR REPORTING COMPLIANCE OF THE SERVICE LEVEL

The Measurement Period will be daily and the Reporting Period will be monthly. Information, such as grief points, termination events and performance statistics against service levels, will be consolidated in the form of a Report and presented at the scheduled monthly meetings. Meetings to be scheduled post award with successful bidder. The supplier will compile a monthly report and deliver the report to the City of Cape Town authorised representative two days prior to the scheduled meeting date.

Communication to be done by the City's delegated Information Technology Manager and authorised representatives from _____ (Company).

5 SERVICE PENALTY

5.1 In each case of a failure to satisfy a Service Level, the Supplier will satisfy the applicable Service Level within seven days from date of notification of service level failure.

5.2 In addition, in each case that a Service Level is not complied with, the City shall be entitled (but not obliged) to recover a Service Penalty, calculated in the manner described in the Service Penalty Calculation Section.

6 SERVICE PENALTY CALCULATION

6.1 Each Service Penalty is made up of an accumulation of Grief Points.

6.2 Grief Points are accumulated automatically by the City due to failures by the Supplier to meet Service Levels.

6.3 Grief points shall be allocated for each failure to meet any Service Levels in each calendar month.

6.4 Each block of 15 (fifteen) Grief Points that is accumulated by the City in each month will constitute a Service Penalty, which may be claimed by the City. Consistently high monthly Grief Points over several months will be reviewed and consideration given to this constituting a Service Level Terminal Event.

6.5 Before every monthly SLA meeting the Supplier will generate a report with all the details of the non-compliance of the service levels and the grief points that the City is entitled.

6.6 The City may claim a Service Penalty by informing the Supplier at the SLA meeting or in writing that it is claiming the Service Penalty.

6.7 On the first accumulation of a Service Penalty, the penalty which may be claimed will be 5% (five percent) of the Order or Service Fee affected that the City must pay the Supplier in terms of this agreement for the month in which the Grief Points were incurred.

6.8 The penalty will be claimed as a discount in following month's account.

6.9 A 12-month rolling period will commence on the first (1st) day of each month. A 12month rolling period is defined as the current month and the previous 11 months.

6.10 At the second accumulation of a Service Penalty in any 12-month rolling period, the penalty that may be claimed will be 10% (ten percent) of the Order or Service Fee affected for the month in which the Grief Points were incurred.

6.11 On the third and subsequent occurrence of a Service Penalty in any rolling 12-month period, the penalty that may be claimed will be 15% (fifteen percent) of the Order or Service Fee affected for the month in which the Grief Points were incurred and may constitute a Service Level Termination Event.

7 TERMINATION – GENERAL EVENTS

7.1 Termination for default: See clause 23 of the GCC
7.2 Termination for insolvency: See clause 26 of the GCC

8 NOTICES

8.1 All notices given by any party to any other hereunder shall be given in writing and shall be sent by prepaid registered post, or shall be delivered by hand, to the recipient's *domicilium* for the time being.

8.2 Notwithstanding anything to the contrary herein contained, a written notice or communication actually received by a party shall be an adequate written notice or communication to him notwithstanding that it was not sent nor delivered to the recipient's chosen *domicilium*.

9 DOMICILIA CITANDI ET EXECUTANDI ADDRESSES

9.1 For all purposes of, and arising in connection with, this Agreement the parties choose as their respective *domicilia citandi et executandi* addresses the above addresses.

9.2 Any party may from time to time change its address for the purpose of this clause to any other address within South Africa upon not less than 10 (ten) days' notice given to the other party to such effect.

10 GENERAL

10.1 This Agreement and the related tender sets out the entire agreement and understanding between the parties in connection with the subject matter hereof and supercedes all prior agreements, if any, between them.

10.2 None of the parties shall be bound by any express or implied term, representation, warranty, promise or the like, not recorded herein.

10.3 No addition to, variation or consensual cancellation of this Agreement, shall be of any force or effect unless in writing and signed by or on behalf of all parties.

10.4 No indulgence which any party may grant to the any other shall constitute a waiver of any of the rights of the grantor who shall not thereby be precluded from exercising any rights against the grantee which might have arisen in the past or which might arise in the future.

10.5 All parties acknowledges that, in entering into this Agreement, they are not relying upon any warranties, representations or undertakings howsoever or to whomsoever made, save and except in so far as same are embodied in this Agreement.

10.6 This Agreement is read together with the General Conditions of Contract and the Special Conditions of Contract as contained in the Tender Document.

11 APPLICABLE LAW

This Agreement shall in all respects be construed in accordance with, and shall be governed by, South African law.

A6 – PRICING SCHEDULE

Schedule D: IT Security Intelligence

Pricing provided must be for a fully working and licensed product. Provide options and fully explain alternatives. Products must be able to integrate into the existing environment. Any ambiguity must be explained as part of the pricing provided. Where additional licenses or modules are recommended to enhance protection, indicate as recommended and not part of the base product. This approach will assist in comparing various technologies.

Sections provided are an indication of anticipated requirements. Where additional sections or components must be added, do so by expanding the table.

1. Price as per below tables.
2. Provide an SLA cost in order to be able to meet the terms and conditions of the service level agreement. All SLA amounts must be provided on an annual basis. If necessary, during evaluation the Bid Evaluation Committee may also divide the Year amounts by 12, in order to determine the appropriate monthly cost.
3. Ad hoc labour costs will be considered for evaluation purposes.
4. Failure to provide pricing for each component of the solution will render the tender nonresponsive, unless the functionality has been included elsewhere within the same section. Do not leave any component blank; an explanation must be provided.

Please indicate the Mark-up percentage: ___5%

Please provide your partnership status by identifying the relevant technology area and your partnership status:

Technology area (Original Equipment Manufacturer)	**Current Partnership Status**
McAfee or equivalent	**Premium**

Schedule A: Reverse Proxy

Preferred service provider: [redacted]

A1	Citrix Reverse Proxy Solution or equivalent				
	Required Item / Description of Item	**QTY**	**Part number**	**Supplier OEM Price ex VAT**	**Mark-up Percentage (%)**
A1.1	1 Year Maintenance Citrix ADC 8905 Premium Edition MPX Appliance or equivalent	4	4049734-GI	R 324 000,00	5%
A1.2	3 Year Maintenance Citrix ADC 8905 Premium Edition MPX Appliance or equivalent	4	4049742-GI	R 810 341,05	5%
A1.3	Citrix ADC 8905 to 8910 upgrade or equivalent	4	3017017-GI	R 140 625,00	5%

A2	Training or equivalent solution				
	Required Item / Description of Item	**QTY**	**Part number**	**Supplier OEM Price Ex VAT**	**Mark-up Percentage (%)**
A2.1	Citrix ADC 12.x Essentials and Traffic Management or equivalent	2		R 49 000.00	0%

[redacted]

A3	Labour Costs – ad hoc						
	Services / Resource Description	**Unit**	Price Year 1 Ex VAT	Price Year 2 Ex VAT	Price Year 3 Ex VAT	Price Year 4 Ex VAT	Price Year 5 Ex VAT
A3.1	Project Manager	Per Hour	R 880	R 880	R 880	R 880	R 880
A3.2	Architect	Per Hour	R 800	R 848	R 898	R 952	R 1009
A3.3	SME (Subject Matter Expert)	Per Hour	R 1 060	R 1 124	R 1 192	R 1 264	R 1 340

A4	Service Level Agreement					
	SLA Description	**Annual Rate (Rand) Year 1 (Excl VAT)**	**Annual Rate (Rand) Year 2 (Excl VAT)**	**Annual Rate (Rand) Year 3 (Excl VAT)**	**Annual Rate (Rand) Year 4 (Excl VAT)**	**Annual Rate (Rand) Year 5 (Excl VAT)**
A4.1	As per SLA	R 63 949	R 67 786	R 71 853	R 76 164	R 80 734

Schedule C: Citric VDI or equivalent

Preferred service provider: [redacted]

C1	Citrix VDI solution or equivalent				
	Required Item / Description of Item	**QTY**	**Part number**	**Supplier OEM Price (Excl. VAT)**	**Mark-up Percentage (%)**
C1.1	Customer Success Services Select - 3 Year- for Citrix Virtual Apps and Desktops Advanced Edition, user / device licenses or equivalent	170	LA-0001911645-38128	R 392 307,69	5 %
C1.2	Customer Success Services Select - 3 Year - for Citrix VPX10 Standard Edition or equivalent	1	LA-0001599891-98564	R 15 230,77	5 %
C1.3	VPX10 Standard Edition or equivalent	1	3013074-GI	R 18 509,00	5 %
C1.4	Customer Success Services Select - 3 Year - for Citrix VPX10 Standard Edition or equivalent	1	4034436-GI	R 11 847,09	5 %

[redacted]

C1.5	Citrix Virtual Apps and Desktops Advanced Edition, user / device licenses or equivalent	100	3013057-GI	R 170 526,32	5 %
C1.6	3 Year - for Citrix Virtual Apps and Desktops Advanced Edition, user / device licenses or equivalent	100	4034301-GI	R 134 626,04	5 %

C2	Labour costs – ad hoc						
	Services / Resource Description	**Unit**	**Price Year 1 (Excl VAT)**	**Price Year 2 (Excl VAT)**	**Price Year 3 (Excl VAT)**	**Price Year 4 (Excl VAT)**	**Price Year 5 (Excl VAT)**
C2.1	Project Manager	Per Hour	R 880,00	R 880,00	R 880,00	R 880,00	R 880,00
C2.2	Architect	Per Hour	R 800,00	R 848,00	R 898,00	R 952,00	R 1 009,00
C2.3	SME (Subject Matter Expert)	Per Hour	R 1 060,00	R 1 124,00	R 1 192,00	R 1 264,00	R 1 340,00

C3	Service Level Agreement					
	SLA Description	**Annual Rate (Rand) Year 1 (Excl VAT)**	**Annual Rate (Rand) Year 2 (Excl VAT)**	**Annual Rate (Rand) Year 3 (Excl VAT)**	**Annual Rate (Rand) Year 4 (Excl VAT)**	**Annual Rate (Rand) Year 5 (Excl VAT)**
C3.1	As per SLA	R 121 963,00	R 129 281,00	R 137 038,00	R 145 260,00	R 153 976,00

A7: SPECIFICATIONS

5.1. Introduction

The City's IS & T department has deployed a variety of IT security technologies and controls as part of the City's IT Security roadmap, in order to ensure confidentiality, integrity and availability of City data.

As part of the previous IT Security Tender 302S/2016/17, a number of technologies that were obsolete have now been replaced with modern technologies. In addition, as part of the previous tender, new technologies have been deployed providing new functionality.

It is therefore the City's intention to expand, support, maintain and mature these newly deployed cyber security environments. These environments are therefore requesting pricing on specific technologies or equivalent as per pricing instruction 4.17.

For new requirements and where no solution has been deployed, service providers may propose solutions that fit the City's defined requirements.

In terms of providing available documentary evidence, details of any additional documentation provided should be included in Schedule 14: List of other documents attached by tenderer, below, and clearly referenced in your answer page/s in its respective answer area. And, where requested in the document, all relevant reference documentation to be attached in Schedule 16, cross referencing the applicable question which should be clearly marked in the document AND within Schedule 16: Information to be provided with the tender.

5.2. IT ARCHITECTURAL STANDARDS AND GUIDELINES

This section provides prospective vendors with technical information regarding the City's current IT environment. For this tender the City's IT Architectural standards are categorized into Compulsory, Preferred and Not Supported for the proposed solutions.

- Compulsory IT Architectural Standards
  These standard are mandatory and the proposed solution(s) must adhere to these standards to ensure interoperability with existing IT landscape and to be accepted by the City's IT Architecture governance.
- Preferred IT Architectural Standards
  These standard are recommended for proposed solution(s) to ensure seamless integration with the City's existing IT landscape and would be

considered for acceptance under the City's current IT Architecture governance.

- Not Supported IT Architectural Standards
  These standard have already been considered under the City's IT Architecture governance framework and rejected or does not comply to the City's standards and therefore must not be considered in the proposed solutions.

5.2.1 Compulsory Minimum IT Architectural Standards

- IP protocol only on the network
- The use of Secure Transport Layer Security (TLS) version 1.2 between all application components
- Encryption of all data in transit which has been classified as confidential, sensitive and personal identifiable information.
- Separate database and application server architecture.
- ODBC or OLEDB connections between applications and databases = Full relational database design, using stored procedures.
- All DLLs must be wrapped as COM+ objects (preferably written in .NET)
- Minimum .Net Framework to be used version 4.7.1 in order to fully support TLS version 1.2 Scheduled events via DTS on SQL Server.
- Application security (i.e. user accounts) at the application or database level (not at the OS level)
- Applications and Databases hosted on Virtual Machine (VM) Servers created using MS Hyper-V (only)
- Solution must function within a Microsoft Managed Environment
- PC thick clients must not function requiring administrative rights
- PC Thick clients must be packable and deployable across a network using System Centre
  Configuration Manager (SCCM) to locked down managed pc's
- Solution interfaces with SAP must be SAP architectural compliant (preferably certified)
- All confidential data must be encrypted
- Applications

5.2.2 Preferred IT Architectural Standards

- Application Solutions hosted on Microsoft platforms
- Web applications rather than thick client/server applications
- If thick client applications are used, these needs to be packaged in the Microsoft Installer format (MSI)
- Business logic implemented in stored procedures rather than in inline code.
- The ability to co-exist with other 3rd party applications on the same hardware.
- Application solutions not hosted on Microsoft platforms but on platforms such as Linux will be reviewed and considered based on the proposal put forward and as it complies with the requirements above

5.2.3 Not Supported IT Architectural Standards

- Active X Controls – the managed desktop environment does not permit these.
- Mapped Network Drives or UNC paths between workstations and application servers
- Mapped Network Drives between application/web/database servers
- Mapped Network Drives or UNC paths between workstations
- IP addressing - use DNS addressing instead
- Application and database on same server
- Custom-developed Windows server services
- User/Application accounts requiring a permanent server login
- Microsoft Access on a server
- Applications written in such a manner whereby usernames and password are embedded in the application code
- Insecure Secure Socket Layer Security (SSL) protocols e.g. SSL version 3

5.3. SCOPE

For this tender it is requires for suppliers to supply and implement the goods and services for the identified 12 sections or technology areas within the IT Security domain. This supply and implementation will happen within the current IT Security operational environment and care must therefore be taken to ensure at all times continued IT Security operations and the no exposure or increased risk is introduced from the program or any individual sub-projects that will be required to deliver on all the tender requirements.

In general, the goods and services scope of the tender includes:

- The solution design, supply and implementation of Hardware components including appliances, storage, servers.
- The solution design, supply and implementation of Software components including application, licensing, subscriptions, maintenance, monitoring tools, management tools etc.
- Services: upgrade, implementation, training, operation, support, maintenance, service level agreements, managed services, security assessments etc.
- Any other interrelated components to ensure a working solution

The specific scopes in the tender in terms of specific solutions or technologies are grouped in twelve solutions sections and include:

- Schedule A: Reverse Proxy

Provide a Citrix or equivalent reverse proxy solution including load balancing and web application firewall functionality as well as reporting and decryption and re-encryption solutions. Delivery metrics for this solution will be managed through agreed Service Level Agreement (SLA)

- Schedule B: Vulnerability Management (VM)

Provide a Tenable vulnerability management solution or equivalent for the infrastructure, application, web application, database and firewall landscape which include reporting and asset classification functionality. Delivery metrics for this solution will be managed through agreed Service Level Agreement (SLA)

- Schedule C: Citrix Virtual Desktop Infrastructure or equivalent

In this section tenderers will be required to expand and provide support and maintenance services for the Citrix VDI platform or equivalent.

- Schedule D: IT Security Intelligence

Tenderers must propose a McAfee solution or equivalent for an IT Security Intelligence Platform to facilitate the integration of the in scope services. Delivery metrics for this solution will be managed through agreed Service Level Agreement (SLA).

Schedule E: Data Loss Prevention

Provide a Data Loss Prevention (DLP) solution which will integrate with the existing environment. The successful tenderer will also be required to project manage the implementation of this solution. Delivery metrics for this solution will be managed through agreed Service Level Agreement (SLA).

- Schedule F: Anti-malware solutions & Email Hygiene

Provide the requested Trend Micro Anti-Malware solution or equivalent for the City's environment. Provide Trend Micro email gateway functionality or equivalent and Exchange 2013 antimalware protection in both Cape Town and Goodwood data centres including advanced anti-spam and anti-malware capability. This solution must also provide reporting for anti-malware, content filtering and spam solutions. Delivery metrics for this solution will be managed through agreed Service Level Agreement (SLA).

- Schedule G: Security assessment services

Security assessment services are required for the CCT's SAP Portal, including application and infrastructure environments and a Microsoft Internet Services project. It is the intention that a panel(s) of service provider for each project will be created. Work will be rotated according to a defined schedule.

- Schedule H: Cloud Access Service Broker (CASB)

Provide a Cloud Access Service Broker (CASB) solution which will integrate with the existing environment and future planned cloud services and applications. The successful tenderer will also be required to project manage the implementation of this solution. Delivery metrics for this solution will be managed through agreed Service Level Agreement (SLA).

5.4. REQUIREMENTS

For each requested solution / goods / service section the background and context is provided followed by the requirements statement for the specific section. Please respond within the table provided per section.

5.5. INFORMATION GUIDE ON FUNCTIONALITY SCORING

In preparing your response to this request, your goal should be to maximise your score by convincing our evaluation and adjudication panels that you offer the best solution and service. Points will be awarded for completeness of responses. You should address all the areas.

Answer each mandatory question in its entirety and insert your responses into Annexures A1-A6 in this document and expand your answers where necessary. Please respond fully to each question before proceeding to the next question. Do not place additional information in an appendix or annexure, rather place any additional answer to the question using the following numbering convention:

If the answer for a question is on page 10, you may append any further answer pages with the question clearly referenced at the top of the page and the page should be numbered 10.1, 10.2, etc. at the bottom of the page (please see positioning and numbering convention of this document);

In terms of providing available documentary evidence, details of any additional documentation provided should be included in Schedule 14: List of other documents attached by tenderer, below, and clearly referenced in your answer page/s in its respective answer area. And, where requested in the document, all relevant reference documentation to be attached in Schedule 16, cross referencing the applicable question which should be clearly marked in the document AND within Schedule 16: Information to be provided with the tender.

If you feel that a question overlaps another question, then repeat your answer as different people may evaluate and adjudicate different answers.

I Schedule A: Reverse Proxy – Background and Requirements

The purpose of this schedule is to expand, support and maintain the Citrix Application Delivery Controller (ADC) which is primary used for reverse proxy, web application firewall and load balancing.

These services are:

- Microsoft SharePoint 2010, 2013 and 2016 web services
- Microsoft Outlook 2013 web access
- Microsoft Lync 2013 / Skype for Business
- SAP Portal web services
- Various other web services
- Citrix VDI published over a HTTPS portal.
- Citrix MDM
- Server publishing
- Secure FTP services using FTP-S and SFTP protocols
- Secure Shell services using SSH

These services are performed through a two tier Demilitarized Zone (DMZ) infrastructure in both the Cape Town and Goodwood Data Centres. Services published may be hosted within the DMZ, or securely published from the corporate network to the Internet. The current DMZ infrastructure does not exist in isolation. There are a number of security devices protecting the City. Where possible, the DMZ firewall architecture will leverage the existing Palo Alto NGFW's, to create multiple DMZs. Within the DMZ a reverse proxy solution is required.

Functional Questions Technical Response

In the following table, please respond to each item. Please complete the "**Description / Technical Response**" column for each item that is included. This section is a technical response section and must be responded in full. An extraction of these question will be repeated as evaluation questions in "Evaluation" section 6.2.1.14 where the scoring criteria will be provided. **It is highly recommended you review the scoring criteria in detail, prior to providing the necessary detailed technical response.**

#	Requirement / Question	Description / Technical Response
A1	Please explain **how** reverse proxy is implemented in the proposed Citrix solution or equivalent and highlight the benefits thereof.	Citrix ADC reverse proxy resides in front of one or more Web servers and shields the origin server from client requests. In the reverse proxy mode, when the appliance receives a request, a virtual server evaluates the request and forwards it to a load balancing virtual server. The incoming request can be transformed by changing the host header or the host URL before it is sent to the backend server. Citrix ADC supports all services listed in the tender document.

A2	Describe in detail how to publish a web service e.g. www.capetown.gov.za from within a back to back firewall topology across two geographically dispersed DMZ's.	To provide access to a web service using Citrix ADC: • Create a load balancer vServer on Citrix ADC located in the DMZ. • Configure vServer IP address. External firewall is configured to NAT traffic from the public network to the IP address. • Add individual internal web services IP addresses to load balance or add a Service Group that contains the IP addresses. • Specify port SSL traffic and bind a SSL certificate to the vServer. • Create an appropriate monitor to verify availability of the back-end web services servers.

		• Communication to the load-balanced web servers originates from the ADC's Subnet IP address directly to the servers located within the DMZ. Where web services are accessible from untrusted or trusted corporate networks from multiple data centres, the Global Server Load Balancing features of Citrix ADC can be leveraged as follows: • Create ADNS listener on each NetScaler ADC pair - DNS clients send DNS queries to the ADNS listeners. GSLB resolves a DNS query into an IP address and returns the IP address in the DNS response. • Create GSLB Sites (aka MEP Listener) - GSLB Sites usually correspond to different datacentres. GSLB Sites are also the IP address endpoints for Citrix ADC's proprietary Metric Exchange Protocol (MEP), which is used by GSLB to transmit proximity, persistence, and monitoring information. • Import Static Proximity DatabaseCitrix ADC includes a database that can be used to determine the geographic allocation of an IP address. Or you can subscribe to a geolocation service and import its database. • Delegate DNS sub-zone to NetScaler ADC ADNS

A3	Describe in detail how to publish a web service e.g. webmail.capetown.gov.za from within the corporate network though a back to back firewall topology across two geographically dispersed DMZ's.	To provide access to a web service using Citrix ADC: • Create a load balancer vServer on Citrix ADC located in the DMZ. • Configure vServer IP address. An external firewall is configured to NAT traffic from the public network to the IP address. • Add individual internal web services IP addresses to load balance or add a Service Group that contains the IP addresses. • Specify port SSL traffic and bind a SSL certificate to the vServer. • Create an appropriate monitor to verify availability of the back-end web services servers. • Communication to the load-balanced web servers originate from the ADC's Subnet IP address through the Internal firewall to the servers located within the corporate network. Where web services are accessible from untrusted or trusted corporate networks from multiple data centres, the Global Server Load Balancing features of Citrix ADC can be leveraged as follows: • Create ADNS listener on each NetScaler ADC pair- DNS clients send DNS queries to the ADNS listeners. GSLB resolves a DNS query into an IP address, and returns the IP address in the DNS response. • Create GSLB Sites (aka MEP Listener)- GSLB Sites usually correspond to different

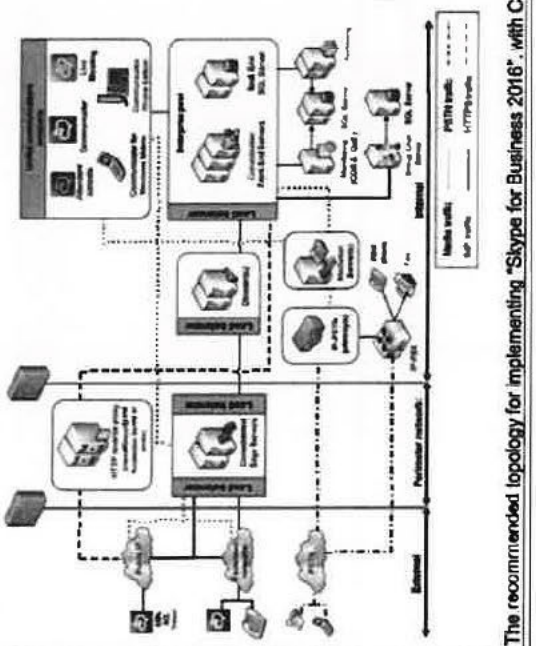
#	Requirement / Question	Description / Technical Response
		data centres. GSLB Sites are also the IP address endpoints for Citrix ADC's proprietary Metric Exchange Protocol (MEP), which is used by GSLB to transmit proximity, persistence, and monitoring information. • Import Static Proximity Database- Citrix ADC includes a database that can be used to determine the geographical location of an IP address. Or you can subscribe to a geolocation service and import its database. • Delegate DNS sub-zone to NetScaler ADC ADNS
A 4	Describe **how** to perform a port redirect for a web service published within the corporate network.	To redirect ports for a web service: • Create a load balancing virtual server and assign the protocol/port and IP address. • Enable the "Protection" advanced settings for the vServer • Configure the redirect URL and port, which redirect traffic to a specific vServer configured on the required port on the ADC.
A 5	Describe **how** to perform a URL redirect **within** the corporate network, and for a URL published to the Internet.	To redirect URLs for a web service: • Create a load balancing virtual server and assign the protocol/port and IP address. • Enable the "Protection" advanced settings for the vServer • Configure the redirect URL, which redirects traffic to a specific vServer configured on the ADC.

A 6	Describe **how** in detail to publish a server from the DMZ to the internal corporate network.	To provide access to servers using Citrix ADC: • Create a load balancer vServer on Citrix ADC located in the DMZ. • Configure vServer IP address. External firewall is configured to NAT traffic from the public network to the IP address. • Add individual internal servers' services IP addresses to load balance or add a Service Group that contains the IP addresses. • Specify port SSL traffic and bind a SSL certificate to the vServer. • Create an appropriate monitor to verify availability of the back-end web services servers. • Communication to the load-balanced web servers originate from the ADC's Subnet IP address through the internal firewall to the servers located within the corporate network.
A 7	Describe **how** in detail to publish a server farm from the DMZ to the internal corporate network.	To access a Citrix Apps and Desktops server farm, a Gateway instance is deployed on the Citrix ADC. • Create a Gateway vServer on Citrix ADC located in the DMZ. • Configure vServer IP address. An external firewall is configured to NAT traffic from the public network to the IP address. • Add individual internal servers' services IP addresses to load balance or add a Service Group that contains the IP addresses. • Specify port for SSL traffic and bind a

#	Requirement / Question	Description / Technical Response
		SSL certificate to the vServer. • Create an appropriate monitor to verify availability of the back-end web services servers. • Configure authentication policies. • Configure Citrix StoreFront and Secure Ticket Authority (STA) settings. • Communication to the Citrix StoreFront, STA servers and Citrix VDA instances originate from the ADC's Subnet IP address through the internal firewall to the servers located within the corporate network.
A 8	In order to securely publish web applications only specific paths may be published. Describe in detail how to perform this task.	The ADC App Firewall feature can be used to implement URL Protection checks to examine request URLs to prevent attackers from aggressively attempting to access multiple URLs (forceful browsing) or using a URL to trigger a known security vulnerability in web server software or web site scripts. The Start URL check examines the URLs in incoming requests and blocks the connection attempt if the URL does not meet the specified criteria. To meet the criteria, the URL must match an entry in the Start URL list, unless the Enforce URL Closure parameter is enabled. The primary purpose of the Start URL check is to prevent repeated attempts to access random URLs on a Web site, (forceful browsing) through bookmarks, external links, or jumping to pages by manually typing in the URLs to skip the pages required to reach that part of the website. Forceful browsing

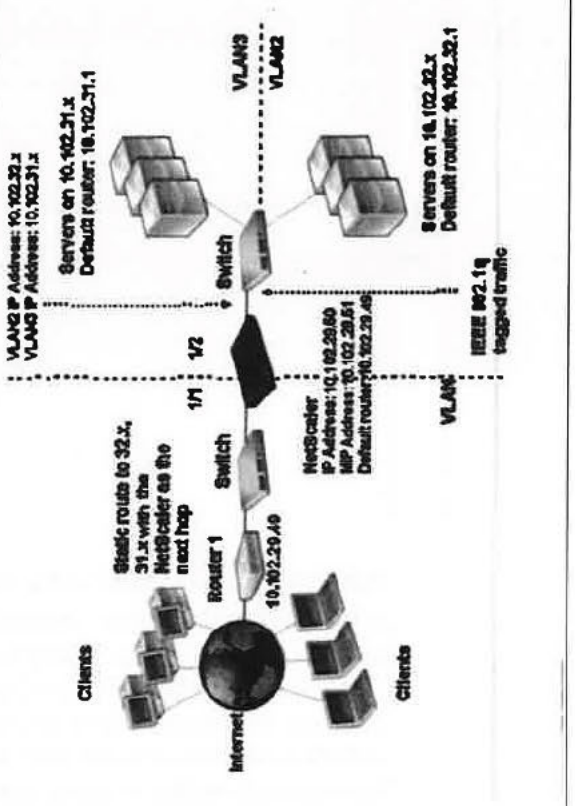
		can be used to trigger a buffer overflow, find content that users were not intended to access directly, or find a back door into secure areas of your Web server. The App Firewall enforces a website's given traversal or logic path by allowing access to only the URL's that are configured as start URLs.
A 9	How do you implement caching and compression for web services published to the corporate network and Internet in order to facilitate acceleration	Both features require minimal configuration and are enabled from the Citrix ADC interface. Citrix ADC Caching feature: The integrated cache provides in-memory storage on the NetScaler appliance and serves Web content to users without requiring a round trip to an origin server. For static content, the integrated cache requires a little initial setup. After you enable the integrated cache feature and perform basic setup (for example, determining the amount of NetScaler appliance memory the cache is permitted to use), the integrated cache uses built-in policies to store and serve specific types of static content, including simple Web pages and image files. You can also configure the integrated cache to store and serve dynamic content that is usually marked as non-cacheable by Web and application servers (for example, database records and stock quotes). Citrix ADC Compression: The compression feature in a NetScaler appliance enables a NetScaler server to compress HTTP responses to compression-

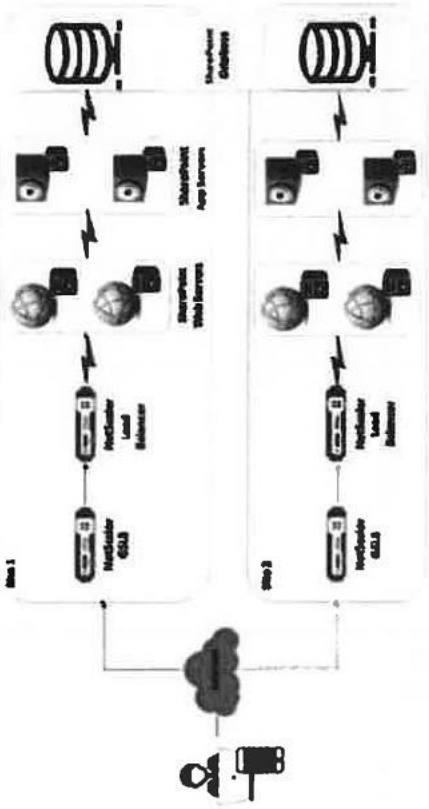
#	Requirement / Question	Description / Technical Response
		aware browsers. Virtually all current web browsers can translate compressed HTTP data. A NetScaler server is configured to compress text in HTML, XML, plain text, CSS (Cascading Style Sheets), and Microsoft Office documents. NetScaler appliance does not compress images in GIF or JPG format. The major benefits of compressed traffic include reduced bandwidth costs, WAN latency reduction, and better server performance.
A 10	How would you implement a reverse proxy solution in conjunction with the Palo Alto NGFWs, using the DMZ's as depicted from these firewalls? All corporate traffic to the DMZ must be inspected by the NGFW and IPS, and all Internet traffic to the DMZ must be inspected by the NGFW and IPS.	All inbound traffic from public networks is inspected by the Palo Alto firewall and directed to IP addresses bound to load balancer or content redirection virtual servers on the Citrix ADC. A public SSL certificate is bound to the VirtualIP address on the Citrix ADC, which decrypts communication and proxies the connection by initiating a connection to servers/services on the corporate network. This traffic originates from the Citrix ADC's Subnet IP (which is not accessible from the public network) and traverses the internal firewall to the corporate servers/services.
A 11	Describe in detail how to publish Skype for Business from a server within the DMZ to the Internet. The following Skype roles are published Lync Edge, Lync Web, SIP, AV and web conferencing.	The diagram below shows the recommended topology for implementing "Microsoft Lync 2013" with Citrix ADC:

#	Requirement / Question	Description / Technical Response
		The diagram below shows the recommended topology for implementing "Microsoft Lync 2013" with Citrix ADC:  The recommended topology for implementing "Skype for Business 2016", with Citrix ADC is as follows:
A 12	Describe in detail how to publish both FTPS and SFTP services from the DMZ to the Internet for external providers to connect to in a secure manner using a digital certificate.	All inbound FTPS and SFTP traffic from public networks traverse the external firewall and are directed to IP addresses bound to load balancer or content redirection virtual servers that are configured to process FTPS and SFTP traffic on the Citrix ADC. Context switch virtual servers can be configured to distribute traffic based on the traffic type and reduce the number of required public IP addresses. Device certificates can be enabled on the virtual server and used to ensure that only authorized devices can connect. One can also require the device certificate when using pre-authentication or advanced

		endpoint analysis policies. The Citrix ADC communicates with the FTPS and SFTP back-end services on the corporate network through the Citrix ADC's Subnet IP to traverse the internal firewall to the corporate servers / services.
A 13	Describe in detail how to publish a SAP Portal to the internet in a secure manner e.g. https://eservices.capetown.gov.za/irj/portal/	SAP is securely accessed from public networks by implementing Load Balancing (SSL offload), Application Firewall and Integrated Caching. Summary of deployment Steps: a) Create load balancing virtual server (SSL offload). b) Create a service for local virtual server. c) Define monitor for service. d) Create signatures for the application firewall and enable the built-in rules in the web-iis category. e) Create an application firewall profile. f) Configure the profile's security checks to enable Buffer Overflow, XSS and SOL Injection protections. g) Configure the profile's settings to bind signatures and exclude file uploads from inspection, to prevent false positives. h) Create an application firewall policy with an expression that identifies the traffic flowing to and from the application, and an action that applies the configured profile's protections to the traffic.

#	Requirement / Question	Description / Technical Response
		i) Bind the policy to the load balancing virtual server. j) Monitor logs and tweak the configuration. Deploy relaxation rules to avoid false positives if needed. k) Optimization (Configure Integrated caching) l) Define Cache Content group and Cache Policy m) Bind the Policy to load balancer n) Monitor logs and Cache object details
A 14	The City currently uses VLAN tagging as a technique to segregate service providers within a Third Party hosted DMZ. This is today configured on the network switch as well as on the Palo Alto firewall. This ensures that that the server is not visible to other service providers within the third Party hosted DMZ. As part of your solution proposal; how would you provide the same or better level of security?	Citrix ADC appliance supports Layer 2 port and IEEE 802.1q tagged VLANs. VLAN configurations are useful when you need to restrict traffic to certain groups of stations. You can configure a network interface as a part of multiple VLANs by using IEEE 802.1q tagging. You can configure VLANs and bind them to IP subnets. The Citrix ADC then performs IP forwarding between these VLANs (if it is configured as the default router for the hosts on these subnets). Port-Based VLANs: The membership of a port-based VLAN is defined by a set of network interfaces that share a common, exclusive Layer 2 broadcast domain. You can configure multiple port-based VLANs. • Tagged VLANs: 802.1q tagging (defined in the IEEE 802.1q standard) allows a networking device (such as the Citrix ADC) to add information to a frame at Layer 2 to identify the VLAN membership of the frame. Tagging allows network environments to

#	Requirement / Question	Description / Technical Response
		have VLANs that span multiple devices. The diagram below illustrates a configuration with multiple VLANs with 802.1 Tagging:
		
A 15	The City's Internet site www.capetown.gov.za is deployed as a Microsoft SharePoint 2013 failover cluster across both Data Centre's Internet Hosting DMZs. How would your proposed solution enable the communication of servers from DMZ to DMZ, across the corporate network?	The topology for a Global Server Load Balancing (GSLB) deployment for SharePoint 2013 across data centres is as follows:



The deployment is the same for both internal and external clients. DNS view helps in managing internal and external IP address mapping with DNS name.

Communication process: 1. A user accesses the www.capetown.gov.za SharePoint login page using a web browser. A DNS request for it is issued.

2. This domain name is bound to GSLB virtual server. So, the resolution request comes to GSLB virtual server which resolves the domain name to an IP address based on

		the GSLB method configured. 3. The IP address of load balancing virtual server is sent to the client depending on whether the user is in the intranet or connecting via the Internet. 4. The client connects to a load balancing virtual server which connects to one of the backend SharePoint web servers depending on the local load-balancing method configured on it. 5. SharePoint web server connects to the appropriate SharePoint app server. An app server takes the request from a web server, does central administration and connects to the backend database for request fulfilment. 6. App server sends the result to the frontend web server which sends it back to the client via NetScaler load balancer.
A 16	The City's Internet site www.capetown.gov.za is deployed as a Microsoft SharePoint 2013 failover cluster across both Data Centre's Internet Hosting DMZs. How would your proposed solution provide load balancing from (a) corporate network and (b) the Internet	Citrix ADCs in both data centres are configured to process SharePoint traffic. All inbound SharePoint traffic from public networks traverse the external firewall and are directed to IP addresses bound to load balancer or content redirection virtual servers that are configured to process SharePoint traffic on the Citrix ADC. The Citrix ADC communicates with the SharePoint back-end services on the corporate network through the Citrix ADC's Subnet IP to traverse the internal firewall. For traffic from the corporate network to

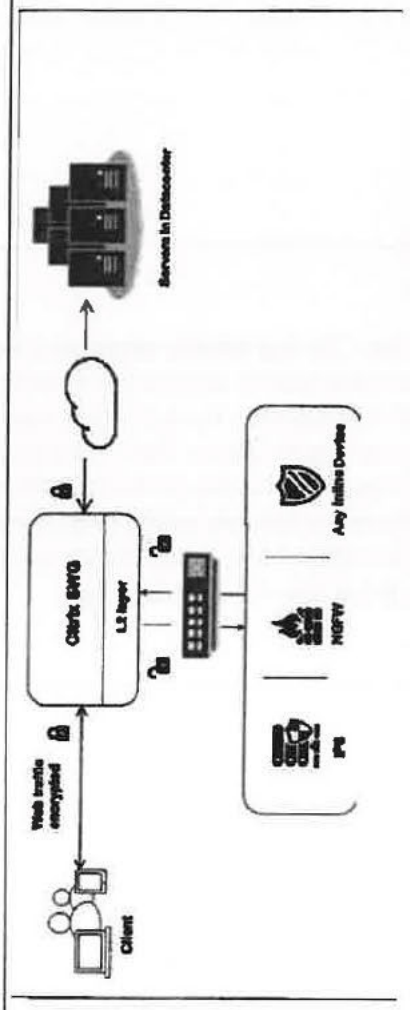
		SharePoint, firewall ports to the NetScaler ADC Virtual IP addresses may be opened if security policies allow for it. Alternatively, internal Citrix ADC instances should be deployed.
A 17	Describe in detail how your solution would provide protection against a distributed denial of service attack from the Internet. Assume all other security controls i.e. firewall has failed to respond appropriately.	Citrix ADC has a HTTP Denial of Service (DoS) Protection feature to protect against DDos attacks. When the NetScaler appliance detects an attack, it responds to a percentage of incoming requests with a Java or HTML script containing a simple refresh and cookie. (You configure that percentage by setting the Client Detect Rate parameter.) RealWeb browsers and other Web-based client programs can parse this response and then resend a POST request with the cookie. DoS clients drop the NetScaler appliance's response instead of parsing it, and their requests are therefore dropped as well. Even when a legitimate client responds correctly to the NetScaler appliance's refresh response, the cookie in the client's POST request may become invalid in the following conditions: • If the original request was made before the NetScaler appliance detected the DoS attack, but the resent request was made after the appliance had come under attack. • When the client's think time exceeds
		four minutes, after which the cookie becomes invalid.

A 18	The City's Internet Service Provider (ISP) strategy provides for the capability to use which ever ISP it prefers, based upon appropriate performance and cost metrics. The City has registered an Autonomous System Number (ASN) with AfriNIC in order to publish the City's address space. How will your proposed solution enable the City to readily switch between ISPs for published services?	A DMZ with internal Virtual IP Addresses on Citrix ADCs should be accessible from multiple Internet providers. There would be a different NAT for each Internet circuit since they are typically different public IPs. To make this work, one would configure GSLB to resolve a single DNS name to multiple public IPs: 1. Create an ADNS service on the NetScaler. NAT it to a public IP on each Internet provider. In your public DNS, create a Host record (A record) for each ADNS public IP. 2. Create one GSLB site (Local). 3. Create GSLB services for each Public IP (one for each Internet provider) that is NATed to the application VIP. 4. Create one GSLB vServer. Bind the DNSname. Bind the two GSLB services. GSLB Persistence is optional. 5. In your public DNS, delete the existing DNS name for the application, create a new DNS delegation (NS records) that delegate the application DNS name to the two NetScaler ADNS services.
		The DNS request can reach the Citrix ADC through either of the Internet circuits. GSLB will respond with either of the GSLB services which are public IPs for the service.

A 19	Describe how to deploy Web Application Firewall (WAF) functionality. Describe in detail your proposed solutions functionality and capabilities in terms of WAF.	Citrix ADC provides the App Firewall feature which offers a comprehensive security solution. The feature is included with Platinum level licensing and can be added to Enterprise licensing as an option. The Citrix ADC Hybrid Security model allows one to take advantage of both a positive security model and a negative security model to come up with a configuration ideally suited for your applications. • Positive security model protects against Buffer Overflow, CGI-BIN Parameter Manipulation, Form/Hidden Field Manipulation, Forceful Browsing, Cookie or Session Poisoning, Broken ACLs, Cross-Site Scripting (XSS), Command Injection, SOL Injection, Error Triggering Sensitive Information Leak, Insecure Use of Cryptography, Server Misconfiguration, Back Doors and Debug Options, Rate-Based Policy Enforcement, Well Known Platform Vulnerabilities, Zero-Day Exploits, Cross-Site Request Forgery (CSRF), and leakage of Credit Card and other sensitive data. • Negative security model uses a rich set signature to protect against L7 and HTTP

		application vulnerabilities. The Web App Firewall is integrated with several third-party scanning tools, such as those offered by Cenzic, Qualys, Whitehat, and IBM. The built-in XSLT files allow easy importation of rules, which can be used in conjunction with the native-format Snort based rules. An autoupdate feature gets the latest updates for new vulnerabilities.
A 20	The City currently uses the Tenable.SC Vulnerability Management suite including the Web Application Scanning (WAS) module. Using a WAS or similar application vulnerability management report for a web application, how would you implement a control to mitigate a SQL injection vulnerability.	Citrix ADC provides the following XML Protection checks provided by the Web App Firewall feature: • XML Format Check • XML Denial of-Service Check • XML Cross-Site Scripting Check • XML SOL Injection Check • XML Attachment Check • Web Services Interoperability Check • XML Message Validation Check • XML SOAP Fault Filtering Check XML Protection checks examine requests for XML-based attacks of all types. XML security checks apply only to content that is sent with an HTTP content-type header of texUxml. If the content-type header is missing, or is set to a different value, all XML security checks are bypassed. Example:HTML SOL injection check • The XML SOL injection check examines the user requests for possible XML SOL Injection attacks. If it finds injected SQL in XML payloads, it blocks the requests.

#	Requirement / Question	Description / Technical Response
		• The Citrix Web App Firewall inspects the presence of SQL keywords and special characters to identify the XML SOL Injection attack. A default set of keywords and special characters provides known keywords and special characters that are commonly used to launch XML SQL attacks.
A 21	The City has widely deployed the use of encryption to secure confidential data in transmission for the City's web site and applications. The City wishes to inspect this data at the NGFW and IPS layer for threats, whilst maintaining the security of the data. Please explain in detail how to achieve this.	The NGFW can be integrated as an inline device with Citrix ADC. A SSL forward proxy appliance can be integrated with one or more inline devices to prevent threats and provide advanced security protection. The inline device can be any security device, such as IPS and NGFW. The following diagram shows how a SSL forward proxy is integrated with inline security devices:



When you integrate inline devices with SSL forward proxy appliance, the components interact as follows:

1. A client sends a request to a SSL forward proxy appliance.

2. The appliance sends the data to the inlinedevice for content inspection based on the policy evaluation. For HTTPS traffic, the appliance decrypts the data and sends it in plain text to the inline device for content inspection. If

#	Requirement / Question	Description / Technical Response
		there are two or more inline devices, the appliance load balances the devices and sends the traffic. 3. The Inline device inspects the data for threats and decides whether to drop, reset, or send the data back to the appliance. 4. If there are security threats, the device modifies the data and sends it to the appliance. 5. For HTTPS traffic, the appliance reencrypts the data and forwards the request to the backend server. 6. The backend server sends the response to the appliance. 7. The appliance again decrypts the data and sends it to the Inline device for inspection. 8. The inline device inspects the data. If there are security threats, the device modifies the data and sends it to the appliance. 9. The appliance re-encrypts the data and sends the response to the client

A 22	Considering the above question, what is the impact, as below: a. Transaction in progress b. Integrity of the encrypted data c. Web application	To provide advanced security protection, a Citrix ADC appliance is integrated with one or more inline devices: Inspecting encrypted traffic. Most IPS and NGFW appliances bypass encrypted traffic, thereby leaving servers vulnerable to attacks. A Citrix ADC appliance can decrypt
		traffic and send it to inline devices for inspection. This enhances the customer's network security. • Offloading inline devices from TLS/SSL processing. TLS/SSL processing is expensive, and this issue can result in high system CPU in IPS or NGFW appliances if they decrypt the traffic. As encrypted traffic is growing at a fast pace, these systems fail to decrypt and inspect encrypted traffic. Citrix ADC helps in offloading inline devices from TLS/SSL processing. This results in an inline device supporting a high volume of traffic inspection. • Loading balancing inline devices. The Citrix ADC appliance load balances multiple inline devices when there is a high volume of traffic. • Smart selection of traffic. Every packet flowing into the appliance might be content inspected, for example, download of text files. User can configure the Citrix ADC appliance to select specific traffic (for example .exe files) for inspection and send the traffic to inline devices for processing the data.

#	Requirement / Question	Description / Technical Response
A 23	Explain in detail how your proposed solution integrates into the existing McAfee ESM solution.	Citrix ADC integrated into McAfee Enterprise Security Manager (ESM) as follows: • Citrix ADC is added as a data source to a to McAfee ESM receiver. • Citrix ADCs are configured to add the McAfee Event Receiver's IP address and port as Syslog server to the ADC's auditing settings. A policy is created and bound on the ADC to send all logs to the McAfee Event Receiver.
A 24	Explain in detail how your proposed solution integrates into your proposed, or other, Data Loss Prevention tools.	Citrix ADC integrates with McAfee products to provide Data Loss Prevention (DLP). It can send traffic over plain text to any security device that can act as an ICAP server. With this capability, one add DLP, AV, or any security device to your deployment without making vital changes.
A 25	Explain in detail the end to end support model from the reseller to the vendor, ensuring that the City has the necessary local support to ensure compliance with the SLA as attached to the tender document.	This is outline in the service management governance document-Appendix J
A 26	Provide details regarding product license and annual license requirements to ensure product maintains latest relevant versions.	To support the features noted in the Reverse Proxy schedule, Platinum licensing is required. Citrix ADC is licensed based on required throughput.

A 27	Provide signed reference letters from companies or organisations with in South Africa where you have provided architecture, implementation and support services for the proposed solution. Only official letters will be recognised which have been authorised by a delegated manager. Contact details must be provided in order to perform verification of your solution. It would be highly beneficial for the reference letters to include details of the project including relevant technologies which the City uses. Provide all required evidence in **Schedule 16: Information to be provided with the tender**	Included in Schedule 16

Schedule C: Citrix Virtual Desktop Infrastructure or equivalent

This section of the tender will facilitate the purchase of software and licenses, including support, maintenance and/or upgrades for the current Virtual Desktop or equivalent solution implemented
at the City. The proposed solution must meet the architectural standard set forth by the Information Systems and Technology (IS&T) department.

Current Environment

The City currently has a VDI implementation with 150 user base which is used to provide a service of publishing corporate applications of which the intended user body are mainly labour broker assigned contractors and external auditors with own devices. A standard set of corporate applications are published to these users which allows access to email, SharePoint, corporate internet, and the SAP application. Access to the VDI portal is available internally via the corporate network as well as externally via public internet.

Future Requirements

The following requirements must to be considered and any solution would need to provide, cater for, or able to scale for deliver such services:

1. The City has revised its Microsoft Enterprise Agreement (EA) in order to save licencing costs and is embarking on an alternate desktop strategy. It is envisaged that these changes will require a greater leverage on VDI to deliver or present corporate applications to any device and required the solution to be operating system agnostic.

2. The City has for a number of years been using a traditional Microsoft Windows desktop (which is currently Microsoft Windows 10 64 bit Professional), with applications installed locally on the desktop. Any solution must have the ability to deliver virtualised applications to the existing environment, or deliver virtualised applications to non-windows desktops.

3. Any proposed solution should take licensing implications into account especially with regard to the change in Desktop EA.

Intent of Tender

The intent of the tender is to provide for expansion, services, licensing, support and maintenance, for the current Citrix VDI installation or equivalent.

Mandatory Requirements for Citrix Virtual Desktop Infrastructure or equivalent

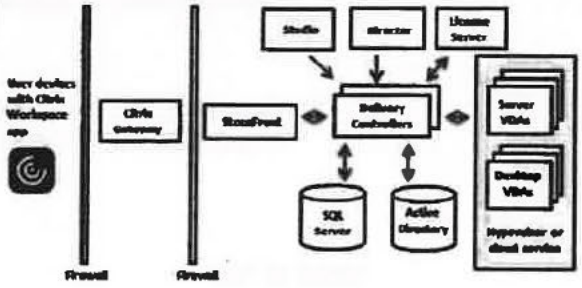
Provide evidence for below requirements in Schedule 16. Failure to do so will render the submission nonresponsive for this schedule.

1. Certified staff in your direct employ. Provide copies of certifications in annexure.
2. The City requires that all licences must be concurrent or enterprise in nature. Does your licensing model provide for this? Provide proof of licensing or equivalent.
3. Your company must be certified to sell Citrix VDI products or equivalent? Provide copies of certifications in annexure.

Functionality Questions

In the following table, please respond to each item. Please complete the "**Description / Technical Response**" column for each item that is included. This section is a technical response section and must be responded in full. An extraction of these

question will be repeated as evaluation questions in "Evaluation" section 4.5 where the scoring criteria will be provided. It is highly recommended you review the scoring criteria in detail, prior to providing the necessary detailed technical response.

#	Technical Requirements / Questions	Description / Technical Response
C 1	Describe how the proposed solution would be able to deliver desktops/applications to the end user by providing dedicated OS per user (dedicated or persistent desktop) and by sharing the Operating System resources on the Server (shared hosted desktop)	This illustration shows the key components in a typical deployment.  VDI Models • Hosted Apps - Delivers only the application interface to the user. • Shared Desktop - Multiple user desktops are hosted from a single, server-based operating system. • Pooled Desktop- Provides each user with a random, temporary desktop operating system.
		Applications and desktops are presented to users using StoreFront which authenticates users access based on AD security groups. Applications are presented via the Citrix workspace application or using a web-based application front end. Multiple operating system instances are provisioned from standardized golden images using Citrix Provisioning or Machine Creation Services.

C 2	Describe how the proposed solution would optimize the usage of server resources and should support network efficient protocols which are capable of delivering the desktops efficiently and effectively consuming minimum bandwidth (30-40 KBPS per desktop).	Bandwidth utilization depends on the type of user and how active users display protocols can be configured to optimize user experience based on network and latency conditions. Streaming
C 3	Describe how the proposed solution would be capable of load balancing and providing the Desktop delivery by internal load balancing algorithms. The same solution should be capable of providing secure access over WAN using SSL or IPSEC VPN technology	Citrix Virtual Apps and Desktops manages user load across multiple identically configured OS instances based on CPU and Memory utilisation by default. Criteria such as Concurrent login tolerance, disk usage, maximum number of sessions can be included if required.
C 4	Describe how the proposed solution integrates with all known vendors offering device certificates, as a measure ensuring certified devices access central systems	When user log on, you can require device certification as part of the authentication process. Citrix Gateway supports device certificates that enable you to bind the device identity to a public key. Devices must use X.509 certificates
C 5	Describe the supported mainstream protocols. At a minimum the following protocols must be support – RDP, PCoIP, ICA /HDX, RemoteFX	Display protocols are vendor dependent. Citrix supports the ICA / HDX display protocol.

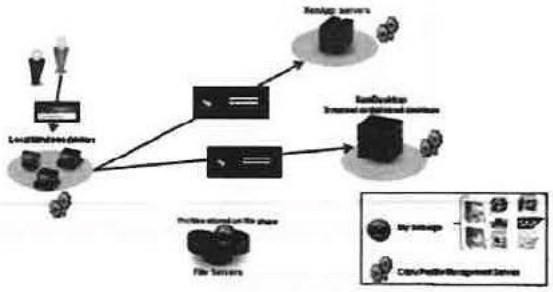
C 6	Describe the different methods of Desktop Delivery like Hosted Share, VDI, Streamed Desktop etc. with single product. Management of all delivery types should be from single console.	The following list provides a brief explanation of Citrix Desktop and Application delivery models. Management of these is performed from a single Citrix Studio console. • Hosted Apps– The hosted apps model delivers only the application interface to the user. This approach provides a seamless way for organizations to deliver a centrally managed and hosted application into the user's local PC. Hosted apps include a few variants: 0 Windows Apps -The Windows apps model utilizes a server-based Windows operating system, resulting in many users accessing a single VM model. 0 VM Hosted Apps - The VM hosted apps model utilises a desktop-based Windows operating system, resulting in a single user accessing a single VM model. This model is often used to overcome application compatibility challenges with a multi- user operating system. 0 Linux Apps - The Linux apps model utilizes a server-based Linux operating system, resulting in many users accessing a single VM model. 0 Browser Apps - The browser apps model utilizes a server-based Windows operating system to deliver an app as a tab within the

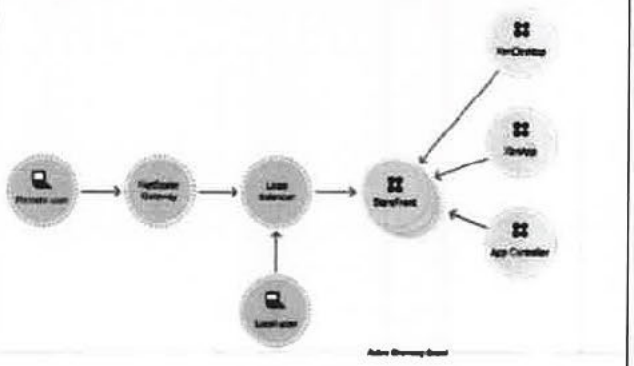
#	Technical Requirements / Questions	Description / Technical Response
		user's local, preferred browser. • Shared Desktop -- With the shared desktop model, multiple user desktops are hosted from a single, server-based operating system. The shared desktop model provides a low- cost, high-density solution; however, applications must be compatible with a multi-user serverbased operating system. Also, because multiple users share a single operating system instance, users are restricted from performing actions that negatively impact other users, for example installing applications, changing system settings and restarting the operating system. • Pooled Desktop - - The pooled desktop model provides each user with a random, temporary desktop operating system. Because each user receives their instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, pooled desktops remove the requirement that applications must be multi-user aware and support server-based operating systems. • Personal Desktop - - The personal desktop model provides each user with a statically assigned, customizable, persistent desktop operating system. Because each user receives their instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. • Pro Graphics Desktop– The pro graphics desktop model provides each user with a hardware-based graphics processing unit

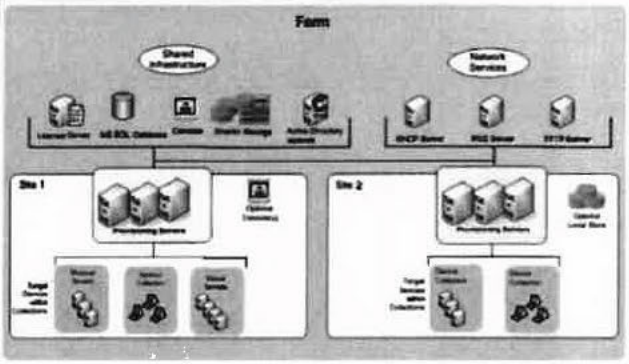
#	Technical Requirements / Questions	Description / Technical Response
		(GPU) allowing for higher-definition graphical content. • Local Streamed Desktop –The local streamed desktop model provides each user with a centrally managed desktop, running on local PC hardware • Local VM Desktop –The local VM desktop model provides each user with a centrally managed desktop, running on local PC hardware capable of functioning with no network connectivity. • Remote PC Access - - The remote PC access desktop model provides a user with secure remote access to their statically assigned, traditional PC. This is often the fastest and easiest VDI model to deploy as it utilizes already deployed desktop PCs.

C 7	Describe how the service level are assured through end session monitoring within the product.	Director uses a troubleshooting dashboard that provides real-time and historical health monitoring of the Citrix Virtual Apps or Desktops Site. This feature allows you to see failures in real-time, providing a better idea of what the endusers are experiencing. The Dashboard provides an overview of the key aspects of a deployment, such as the status of: • User sessions and session use • Logon performance • Connections and machines, including failures • Load evaluation • Historical trends • Infrastructure Platinum level licensing is required to send automated alerts.

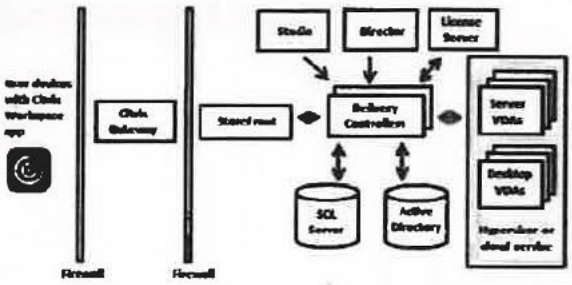
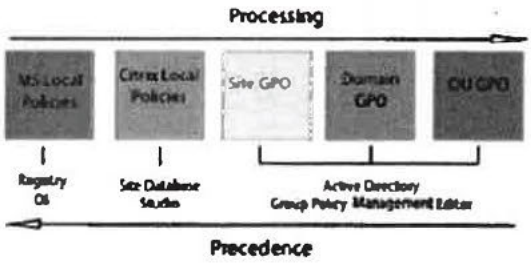
C 8	Describe how profiles are managed	Citrix Profile Management and Workspace Environment Management work hand in hand to manage and optimize the user experience. Citrix Profile Management Profile management ensures that the user's settings are applied to the user's virtual desktop and applications, regardless of the location and endpoint device. Profile management is enabled through a profile optimization service that provides an easy, reliable way for managing these settings in Windows environments to ensure a consistent experience by maintaining a single profile that follows the user. It auto-consolidates and optimizes user profiles to minimize management and storage requirements and requires minimal administration, support and infrastructure while providing users with improved logon and logout. Workspace Environment Management Resource management- To provide the best experience for users, Workspace Environment Management monitors and analyzes user and application behaviour in real-time, then intelligently adjusts RAM, CPU, and I/O in the user workspace environment.

#	Technical Requirements / Questions	Description / Technical Response
		Profile management- To deliver the best possible logon performance, Workspace Environment Management replaces commonly used Windows Group Policy Object objects, logon scripts, and preferences with an agent which is deployed on each virtual machine or server. The agent is multi-threaded and applies changes to user environments only when required, ensuring users always have access to their desktop as soon as possible. 
C 9	Describe how only applications are delivered based on user roles and profiles	StoreFront authenticates users to sites hosting resources and manages stores of applications and desktops that users access. It hosts your enterprise application store, which lets you give users self-service access to app and desktops you make available to them. It also keeps track of users' application subscriptions, shortcut names, and other data to ensure they have a consistent experience across multiple devices. When users connect from outside the corporate firewall, Citrix Cloud can use Citrix Gateway formerly NetScaler Gateway) technology to secure these connections with SSL. Citrix Gateway or the Citrix VPX virtual appliance is an SSL VPN appliance that is deployed in the

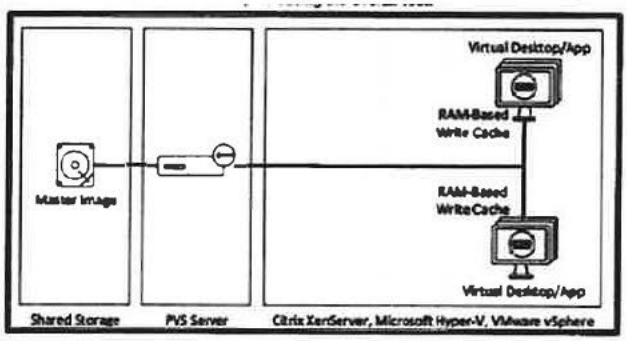
#	Technical Requirements / Questions	Description / Technical Response
		demilitarized zone (DMZ). It provides a single secure point of access through the corporate firewall. Applications and desktops are assigned to specific users or user groups from the Citrix Studio Console. 
C 10	Describe the support for single image provisioning	Citrix Provisioning is a streaming technology that delivers an OS image including applications, patches, updates, and other configuration information to virtual and physical machines. It centralizes virtual machine management while reducing the operational and storage costs of a virtualized desktop environment. Using Citrix Provisioning, any virtual disk can be configured in standard image mode. Standard image mode allows many computers to boot from it simultaneously, greatly reducing the number of images that must be maintained and the amount of required storage. The virtual disk is in a read-only format. Target devices cannot change the image.

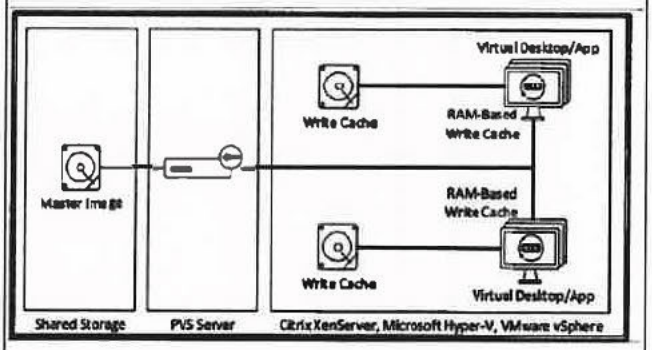
#	Technical Requirements / Questions	Description / Technical Response
		
C 11	Describe how the proposed solution handles the requirement to spawn both persistent and non-persistent desktops from a master image	Provisioning Services streaming technology allows computers to be provisioned and re- provisioned n real-time from a single shared-disk image. This enables administrators to eliminate the need to manage and patch individual systems. Instead, all image management is done on the master image. When you create a machine catalogue for VDI desktops, you create one of these types of desktops: • Random non-persistent desktops, also known as pooled VDI desktops. Each time users log on to use one of these desktops, they connect to a dynamically selected desktop in a pool of desktops based on a master image. All changes to the desktop are lost when the machine restarts. • Static non-persistent desktop. The first time a user logs on to use one of these desktops, the user is assigned a desktop from a pool of desktops based on a master image. After the first use, each time a user logs in to use one of these desktops, the user connects

#	Technical Requirements / Questions	Description / Technical Response
		to the same desktop that was assigned on first use. All changes to the desktop are lost when the machine restarts. • Static persistent, also known as VDI with Personal vDisk. Unlike other types of VDI desktops, these desktops can be fully personalized by users. The first time a user logs on to use one of these desktops, the user is assigned a desktop from a pool of desktops based on a master image. Subsequent logins from that user connect to the same desktop that was assigned on first use. Changes to the desktop are retained when the machine restarts because they are stored in a Personal vDisk
C 12	Describe how the proposed solution delivers a Windows 10 Professional desktop	Windows 10 desktops can be delivered using Citrix Provisioning by creating and configuring a master Windows 10 Target Device vDisk and creating machine catalogues and Windows 10 Desktop VDA instances from the Citrix Studio console based on options noted in section C11.
C 13	Describe how the proposed solution delivers a minimal footprint OS on enduser devices e.g. ThinOS and ZeroOS or equivalent	Delivery of the thin client OS to end-user devices is done by 3rd party non-Citrix vendor-specific products

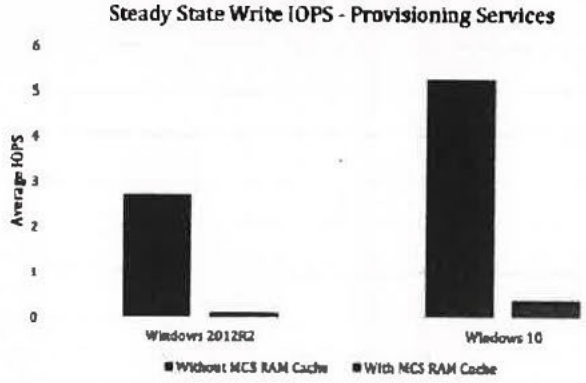
#	Technical Requirements / Questions	Description / Technical Response
C 14	Describe how the proposed solution provides the delivery of applications on any kind of device including tablets	
C 15	Describe how the proposed solution delivers policy based controls (session/printing bandwidth control for every desktop)	Citrix policies are used to control user access and session environments of the control connection, security, printing and bandwidth settings. You can create policies for specific groups of users, devices, or connection types. Computer settings (policy settings applying to machines) define the behaviour of virtual desktops and are applied when a virtual desktop starts. These settings apply even when there are no active user sessions on the virtual desktop. User settings define the user experience when connecting using ICA. User policies are applied when a user connects or reconnects using ICA 

#	Technical Requirements / Questions	Description / Technical Response
C 16	Describe how the proposed solution provides an independent hypervisor	The following hypervisors are supported: • Amazon Web Services (AWS) • Citrix Hypervisor (formerly XenServer) • CloudPlatform (deprecated) • Microsoft Azure Classic (deprecated) • Microsoft Azure Resource Manager • Microsoft System Center VirtualMachine Manager • Nutanix Acropolis • VMware vSphere (vCenter + ESXi) Citrix Hypervisor is the complete server virtualization platform from Citrix. The Citrix Hypervisor package contains all you need to create and manage a deployment of virtual x86 computers running on XenServer, the opensource hypervisor with near-native performance. Citrix Hypervisor is optimized for both Windows and Linux virtual servers. Citrix Hypervisor runs directly on server hardware without requiring an underlying operating system, which results in an efficient and scalable system. Citrix Hypervisor works by abstracting elements from the physical machine (such as hard drives, resources, and ports) and allocating them to the virtual machines running on it.

#	Technical Requirements / Questions	Description / Technical Response
C 17	Describe how the proposed solution delivers advanced features for memory, CPU and disk IOPs management	Citrix Provisioning provides several features to optimize hardware and storage requirements. **VM- Cache In RAM** RAM associated with the virtual machine holds the write cache drives for each target virtual machine. This option provides high performance due to the speed of RAM. However, if the RAM cache runs out of space, the virtual machine will become unusable. To use this option, significant amounts of RAM must be allocated to each virtual machine, increasing the overall cost.  **VM -Cache In RAM with Overflow to Disk** A combination of RAM and local storage is used for the write cache. First, writes are stored within the RAM cache, providing high performance. As the RAM cache is consumed, large blocks are removed from the RAM cache and placed onto the local storage write cache disk. This option provides high levels of performance with the low cost of local storage.



Utilizing this integrated technology reduces write IOPS by 95%



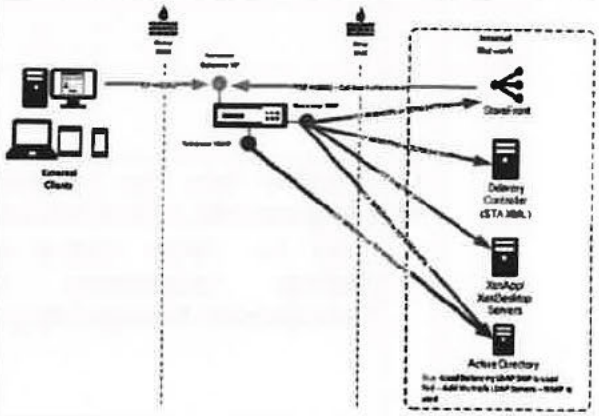
Cache in RAM with Overflow to Disk is the recommended option.

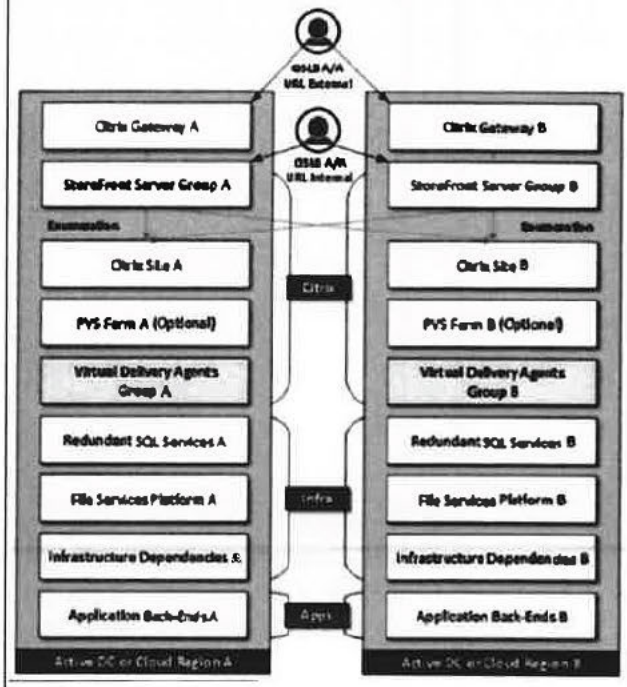
PVS-Accelerator

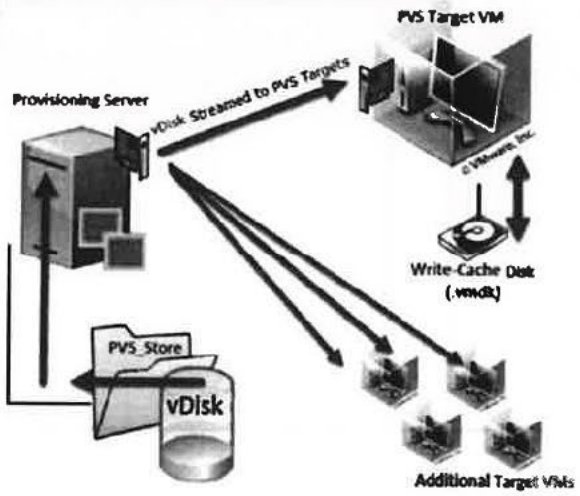
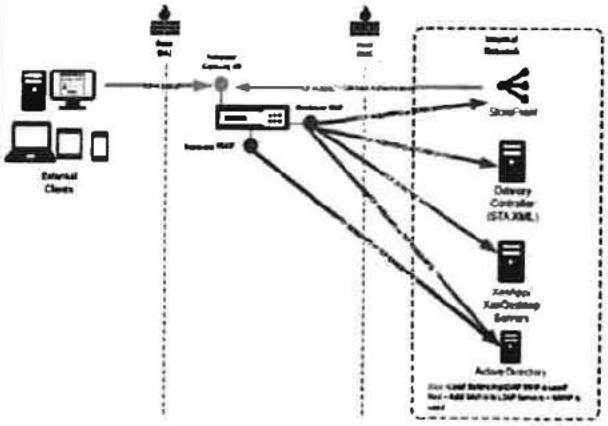
Using PVS-Accelerator virtual appliances dramatically improves the combination of Citrix Hypervisor and Citrix Provisioning. Premium licensing is required for this component

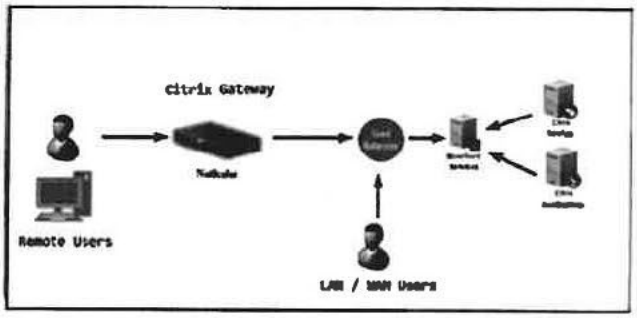
When this feature is enabled, Citrix Provisioning targets device (VM) read requests are cached directly on the Citrix Hypervisor server machine. These requests are cached in physical memory or a storage repository. When subsequent VMs on that Citrix Hypervisor server make the same read request, the virtual disk is streamed directly from cache, not from the Citrix Provisioning server. Removing the need to stream from the Citrix Provisioning server reduces network utilization and processing on the server

#	Technical Requirements / Questions	Description / Technical Response
		considerably. This approach results in a substantial improvement in VM performance.
C 18	Describe how the proposed solution integrates with Active Directory 2012 R2 in order to allow various methods of desktop assignment/ entitlement/ management through City's AD	Citrix Virtual Apps and Desktop components that run on Microsoft OS are all domain-joined. Access to published resources is controlled by assigning AD security groups to allocate resources to users that are grouped based on their requirements. Multiple authentication mechanisms for connections through Citrix Gateway is available including authentication to MS Active Directory and Azure AD. The following authentication types are available: • Lightweight Directory Access Protocol (LDAP/S) • RADIUS • SAML • TACACS+ • Client certificate authentication (including smart card authentication) The diagram below illustrates a deployment where users on public networks authenticate to Active Directory to access published Citrix VirtualApps and Desktops resources.

#	Technical Requirements / Questions	Description / Technical Response
		
C 19	Describe how the proposed solution provides high availability and disaster recovery in order to be able to extend the solution to the DR site whenever the need arises for high availability	Disaster recovery can be implemented in several ways depending on the business' recovery objectives and time allowed to recover. Disaster recovery options: • Recover from Offline Backup • Recover via Replication • Replication with Automated Recovery • Hot Standby (Active-Passive) with Manual Failover • Hot Standby (Active-Passive) with Automated Failover • Active-Active with Automated Failover The diagram illustrates an Active-Active DR scenario that is more seamless to end-users with Automated Failover that leverages Citrix ADC GSLB (Global Server Load Balancing).

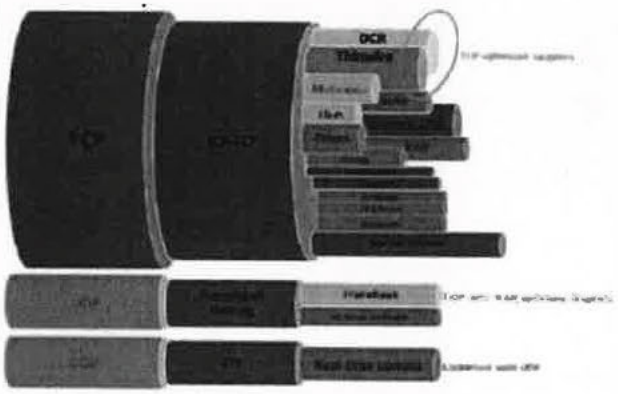
#	Technical Requirements / Questions	Description / Technical Response
		
C 20	Describe how the proposed solution provides scalability without major reconfiguration or redesign	Citrix Virtual Apps and Desktops capacity can be scaled by adding additional virtual machine instances to machine catalogues from the Citrix Studio Console. Citrix Studio can create additional Active Directory machine accounts. It communicates with Citrix Provisioning and the Hypervisor to deploy additional instances that are booted from a generalized OS image without requiring additional OS and application configuration. The hypervisor must have enough processors, memory and storage available to accommodate additional machines.

#	Technical Requirements / Questions	Description / Technical Response
		
C 21	Describe how the proposed solution supports secure gateway connections or proxy connections through firewall – standard firewall ports to be used	Citrix Gateway is used to provide secure access from untrusted networks to resources on trusted networks. Licensing is available to deploy it to standalone physical or virtual appliances and the feature is also available on appliances with Citrix ADC licensing. Access to Citrix Virtual Apps and Desktops resources are provided by configuring the Gateway instance for ICA proxy mode or by configuring SmartAccess which allows one to do pre-authentication checks to control access to resources using Citrix Gateway session policies. 

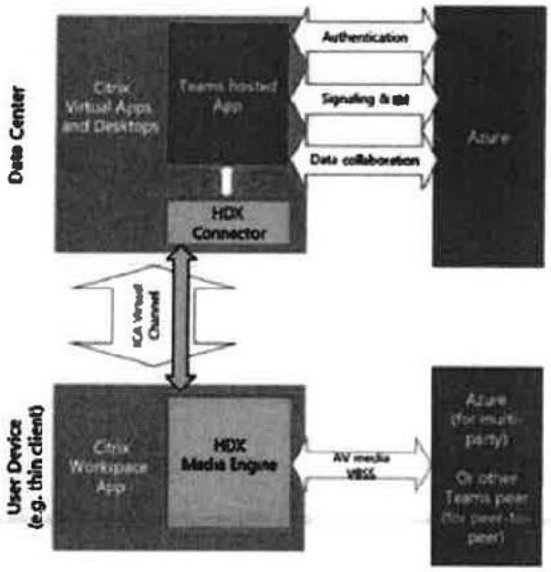
#	Technical Requirements / Questions	Description / Technical Response
C 22	Describe how the proposed solution supports connectivity via LAN, WAN and internet	Users can connect to the Virtual Apps and Desktops environment from: • Public networks - User connections are facilitated by Citrix Gateway to provide secure access by proxying all HDX connections. • LAN - Users on trusted LAN networks can connect directly to resources or through Citrix • WAN- Users on trusted WAN networks. can connect directly to resources or through Citrix Gateway if required. The Citrix policies may be configured to optimize the display protocol for these connections. 

C 23	Describe how the proposed solution provides bandwidth optimisation capabilities, both manual and automated for fast and slow networks from connected devices	Selecting the correct display protocol determines the quality of static images, video and text within user's session as well as determining the impact on single server scalability and network utilization. Administrators have the following options: optimisation capabilities, • Legacy - optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+). both manual and automated for fast and • Desktop Composition Redirection - offloads desktop Windows manager DirectX commands to slow networks from the endpoint, but only supports a Windows desktop VDA. Plus, in the

		7.15 LTSR release, connected devices Desktop Composition Redirection is a depreciated feature. • Framework- a UDP-based protocol that can provide high refresh rates in environments with high latency and high packet loss scenarios at the cost of greater network bandwidth utilization, commonly found on broadband wireless connections. • H.264- Often referred to like the video codec, which provides the highest frame rates required for the high-quality video while saving network bandwidth. It does come at the expense of CPU processing time, reducing single server scalability. H.264 is the preferred codec when users predominately use multimedia applications. • Thinwire - Based on the original Citrix patents from the 1990s that thinly transfers data over a wire. Use Thinwire in the majority of use cases as it provides a good user experience with minimal resource costs. There are two variations of Thinwire. o Legacy- optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+). o Thinwire+ - optimized for Desktop Windows Manager (DWM) graphics engine in Windows 8, Windows 10, Windows 2012 and Windows 2016 • Selective H.264 (Adaptive Display)- utilizes multiple codecs (H.264 and Thinwire+) simultaneously for portions of the screen o Do not use - only uses Thinwire+ and not H.264. Best for users without server-rendered

#	Technical Requirements / Questions	Description / Technical Response
		video or other graphically intense applications. o For the entire screen - Only uses H.264. Best for users with heavy use of server- rendered video and 3D graphics, especially in low-bandwidth situations. o For actively changing regions- Uses H.264 for the portions of the screen that are constantly changing while the remainder of the screen uses Thinwire+. This is the best option for most users.  **Optional: Citrix SD-WAN** Citrix SD-WAN appliances may be used as a WAN Edge solution to optimize network traffic including Citrix HDX/ICA traffic.SD-WAN is not included in Citrix Virtual Apps and Desktops licensing. Citrix SO-WAN can parse the ICA protocol to provide Quality-of-Service (QoS) and deep visibility into the HDX traffic. It splits ICA channels into multiple streams (real-time, interactive, bulk, and background), even over a single port, to allow for prioritization and steering of each stream. Granular awareness of the protocol allows for a reliable Citrix Workspace experience with efficient and effective delivery

#	Technical Requirements / Questions	Description / Technical Response
		across the WAN. Citrix SD-WAN enables you to monitor HDX session quality by computing a Quality-of Experience (QoE) metric based on network conditions. Fair Sharing of bandwidth between HDX users means the activities of one userstreaming video or large file transfers or print jobs -don't impact other user experiences on the same network link.

C 24	Describe how the proposed solution supports bi-directional video and audio	The Citrix H.264 display protocol often referred to like the video codec, provides the highest frame rates required for the high quality video while saving network bandwidth. It does come at the expense of CPU processing time, reducing single server scalability. H.264 is the preferred codec when users predominately use multimedia applications. Communication for Microsoft Teams and Skype can be optimized by installing Citrix real-time optimization packs to offload video to user devices. 

C 25	Provide signed reference letters from companies or organisations with in South Africa where you have provided architecture, implementation and support services for the proposed solution. Only official letters will be recognised which have been authorised by a delegated manager. Contact details must be provided in order to perform verification of your solution. It would be highly beneficial for the reference letters to include details of the project including relevant technologies which the City uses. Provide all required evidence in **Schedule 16: Information to be provided with the tender**	Included in Schedule 16