



CITY OF CAPE TOWN
ISIXEKO SASEKAPA
STAD KAAPSTAD

Making progress possible. Together.

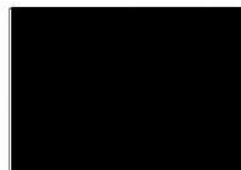
MEMORANDUM OF AGREEMENT

MADE AND ENTERED INTO BETWEEN

CITY OF CAPE TOWN METROPOLITAN MUNICIPALITY

And

NCLOSE (PTY) LTD T/A NCLOSE
(REGISTRATION NO. [REDACTED])



PREAMBLE

WHEREAS Tender 26SS/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 not exceeding 5 years, commencing from the date of commencement of the contract 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**"), herein represented by the [REDACTED] or his **nominee** and duly authorised hereto;

1.2. [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]

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

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 supercede 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.

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

6.6.1 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.

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 Supplier's 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.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

THE CITY OF CAPE TOWN:

Signature:

[Redacted Signature]

Name:

[Redacted Name]

Capacity:

[Redacted Capacity]

Date:

[Redacted Date]

Witness 1:

[Redacted Witness 1]

Witness 2:

[Redacted Witness 2]

SUPPLIER:

[Redacted Supplier Signature]

Signature:

Name:

[Redacted Name]

Capacity:

[Redacted Capacity]

Date:

10 June 2021

Witness 1:

[Redacted Witness 1]

Date: 11.06.2021

Witness 2:

Date:

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

PART A (TO BE FILLED IN BY TENDERER):

1.1 Required Details (Please provide applicable details in full):

(3) FORM OF OFFER AND ACCEPTANCE

TENDER 265S/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)	[REDACTED]

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

- confirms that it has examined the documents listed in the Index (including Schedules and Annexures) and has accepted all the Conditions of Tender;
- confirms that it has received and incorporated any and all notices issued to tenderers issued by the CCT;
- 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;
- offers to supply all or any of the goods and/or tender all or any of the services described in the tender document to the CCT in accordance with the:
 - terms and conditions stipulated in this tender document;
 - specifications stipulated in this tender document; and
 - at the prices as set out in the Price Schedule (Section 4).
- accepts full responsibility for the proper execution and fulfilment of all obligations and conditions in terms of the Contract.

[REDACTED]

Signature(s)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

IN	3
1	

Print name(s)

On behalf of the tenderer (duly authorised)

16/03/2020

Date

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 on 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

[REDACTED]

Print name(s):
(duly authorised in terms of the System
of Delegations as approved by Council)

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.

Subject

Details

.....

.....

.....

Subject

Details

.....

.....

.....

Subject

Details

.....

.....

.....

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 **City of Cape Town**. The address of the Purchaser is **12 Hertzog Boulevard, Cape Town, 8001**.

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.

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. Tenders 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)
- b) 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;
- c) 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;
- d) 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).
- e) 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

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.

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

- 1.12 '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 value adding activities.
- 1.19 'Order' means an official written order issued for the supply of goods or works or the rendering of a service.
- 1.20 'Project site', where applicable, means the place indicated in bidding documents.
- 1.21 'Purchaser' means the 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 anti-dumping 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		NO	X
-----	--	----	---

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.

TENDER NO 265S/2019/2020

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)
			Not Applicable

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 CGT is expected to be transferred out of the Republic? (Please mark with X)

YES	X	NO
-----	---	----

4.1 If YES, furnish particulars below

No Payment will be made or transferred outside of the Republic

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.

Signature
Print name
On behalf of the tenderer (duly authorised)

Date

16/03/2020

TENDER NO:265S/2019/2020

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 0800 32 31 30 (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.

Signature
Print name:
On behalf of the tenderer (duly authorised):

Date

16/05/2020

TENDER NO-265S/2019/2020

Schedule 9: Occupational Health and Safety Agreement

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

.....
(Supplier/Mandatory/Company/CC Name)

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

I,, representing

..... 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 I/We are insured with an approved licensed compensation insurer.

COID ACT Registration Number:

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 on the day of March 2020

.....
Mandatory

Signed at on the day of 20

Witness

.....

for and on behalf of
City of Cape Town

TENDER NO:265S/2019/2020

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: _____ (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 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.

Signature _____

Date

16/03/2020

Name (PRINT)

(For and on behalf of the Tenderer (duly authorised))

A4 - 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



[Company]

(of the other part)

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) of _____ (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 representative by 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
"Commencement date"	structure or employee of the City acting in terms of delegated authority; date of signature of last party hereto or date as agreed 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 honouring 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 hours	working 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 [REDACTED] and [REDACTED] (Company);
Resolution	System is repaired and made operationally available;
Response	Representative from [REDACTED] (Company) arrives on-site or email acknowledgement that [REDACTED] (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"

[REDACTED] (Company), Registration Number: [REDACTED] of physical address: [REDACTED]; Postal address: [REDACTED], a company duly incorporated in accordance with the company laws of South Africa, represented herein by [REDACTED] 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 # N/A, 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 [redacted] (Company)'s authorised representatives, see names below, with an Order number by Fax or email. This number must be reflected on the related invoice. [redacted] (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

[redacted] (Company)'s contact details:

Procurement or orders

Authorised Representative	Name: [REDACTED] Tel number: [REDACTED] Email add: [REDACTED] Fax Num: <u>NA</u>	Provide Percentage of not meeting Service Level (Example 60%) <u>10%</u>
Escalation Level 1	Name: [REDACTED] Tel number: [REDACTED] Email add: [REDACTED] Fax Num: _____	Provide Percentage of not meeting Service Level (Example 80%) <u>10%</u>
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 0%) <u>10%</u>
---------------------------	---	--

Escalation Level 1	Name: [REDACTED] Tel number: [REDACTED] Email add: [REDACTED] Fax Num: [REDACTED]	Provide Percentage of not meeting Service Level (Example 80%) <u>10%</u>
Escalation Level 2	Name: [REDACTED] Tel number: [REDACTED] Email add: [REDACTED] Fax Num: [REDACTED]	

City of Cape Town contact detail:

Procurement

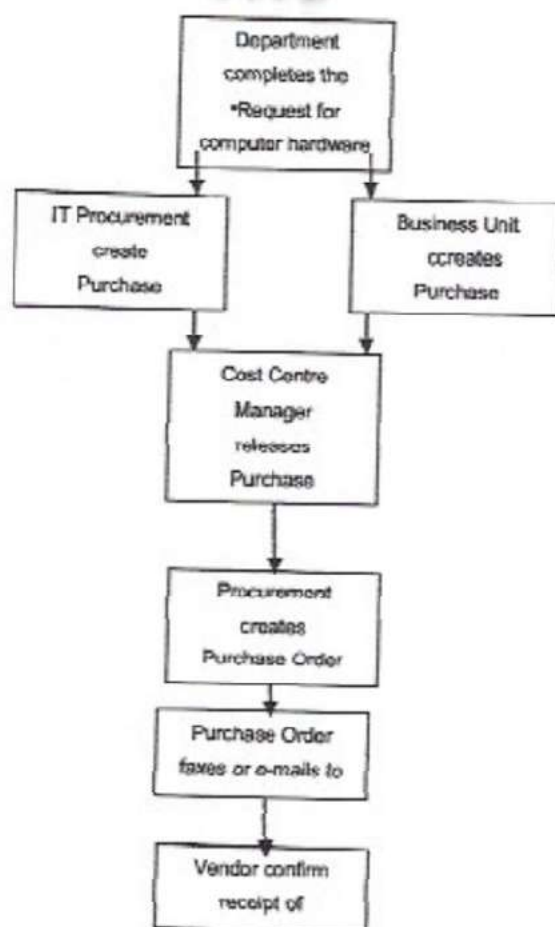
Authorised representative: [REDACTED]

E-Mail address: [REDACTED]

Telephone Number: [REDACTED]

Fax Number: [REDACTED]

City of Cape Town Procurement process:



Warranty Repairs / Services / Fault Reporting

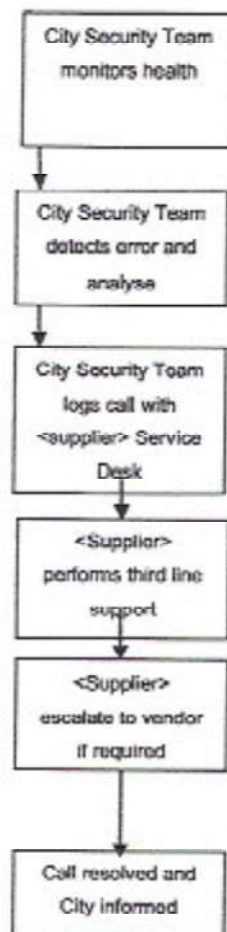
Authorised representative: [REDACTED]

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



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 Provider	Adherence to all change control, maintenance and emergency procedures	Communication with City contacts only
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

		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 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,	Provided within seven (7) full Calendar Days after the last day of	2 Grief Points
#	Service Element	Service Measure	Service Metric	Grief Points incurred for non-performance
		security updates and related recommendations	each month (yes/no) Assessed monthly	
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 Working Days	5 Grief Points
		Maximum Time To Replace (TTR ^{pMax})	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	5 Grief Points

#	Service Element	Service Measure	Service Metric	Grief Points incurred for non-performance
			Note: non-availability of technical support may result in Device and/or Service Unavailability, and will be penalised consequently	
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	Specified items delivered – not defined	--
			Packaging as specified – not defined	--

			Labelling as specified – not defined	–
			Delivery within quoted lead time -	---

3.3 Schedule C: Citrix Virtual Desktop Infrastructure or equivalent

#	Service Element	Service Measure	Service Metric	Grief Points incurred for non-performance
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 (TTR ^{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	5 Grief Points

#	Service Element	Service Measure	Service Metric	Grief Points incurred for nonperformance
			Note: non-availability of technical support may result in Device and/or Service Unavailability, and will be penalised consequently	
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	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	Provided within seven (7) full Calendar Days after the last day of each month (yes/no) Assessed monthly	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 non-performance
---	-----------------	-----------------	----------------	---

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
		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	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	As specified – not defined	---
		Repair or replacement process followed	As specified – not defined	---

#	Service Element	Service Measure	Service Metric	Grief Points incurred for non-performance
---	-----------------	-----------------	----------------	---

		Maximum Time To Restore (TTR ^{Max}) – Priority 1 & 2 Incidents	Not defined	–
		Maximum Time To Replace (TTR ^{pMax})	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

#	Service Element	Service Measure	Service Metric	Grief Points incurred for non-performance
---	-----------------	-----------------	----------------	---

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

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

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 within	1 Grief Point

4 FREQUENCY FOR REPORTING COMPLIANCE OF THE SERVICE LEVEL

15. 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.

16. 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 12-month 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 12month 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 acknowledge 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.

A5 - 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: 10%

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

Technology area (Original Equipment Manufacturer)	Current Partnership Status
Tenable	Silver Reseller

B1	Tenable Vulnerability Management Solution or equivalent				
	Required Item / Description of Item	QTY	Part number	Supplier OEM Price (Excl. VAT)	Mark-up Percentage (%)
B1.1	Tenable SC - On Premise – 2048 Hosts - Scanner(s) Included - Annual Subscription or equivalent	2048	EM-SERV-SC 2048	R 499 262,40	10 %
B1.2	Web Application Scanner	127	TIO-WAS-127	R 576 196,47	10 %

B2	Training or equivalent solution				
	Required Item / Description of Item	QTY	Part number	Supplier OEM Price (Excl. VAT)	Mark-up Percentage (%)
B2.1	Tenable SC or equivalent	2	EM-TRG-VCS SCAN	R 51 300,00	10 %
B2.2	Web Application Scanner	2	Not available	R 0	10 %

B3	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)
B3.1	Project Manager	Per Hour	R 850,00	R 850,00	R 900,00	R 900,00
B3.2	Architect	Per Hour	R 950,00	R 950,00	R 1 000,00	R 1 050,00

B3.3	SME (Subject Matter Expert)	Per Hour	R 950,00	R 950,00	R 1 000,00	R 1 000,00	R 1 050,00
------	-----------------------------	----------	----------	----------	------------	------------	------------

B4 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)	
B4.1	As per SLA	R 34 000,00	R 34 000,00	R 36 500,00	R 36 500,00	R 39 055,00	

Schedule E: Data Loss Prevention

E1 Data Loss Prevention				
	Required Item / Description of Item	QTY	Part number	Supplier OEM Price (Excl. VAT)
Data Loss Prevention				
E1.1	DLP Suite	18000	DLPSU/JP-5-CP12-X-N	R 4 142 482,11
				10 %

E1.2	Initial support maintenance	1	ESESPT-5-CP12-X-N	R 821 136,41	10 %
E1.3	DLP Cloud	18000	DLP-CAIP-5-CP12-X-N	R 2 180 861,05	10 %
	Reporting				
E1.4	Appliance / hardware	18000	ESESPT-5-CP12-X-N	R 327 265,38	10 %
E1.5	Licensing	18000		Included in E1.1 and E1.3	10 %
E1.6	Initial support maintenance and	18000		Included in E1.1 and E1.3	10 %

E2 Project Services						
	Services	Unit	Price Year 1 (Excl VAT)	Price Year 2 (Excl VAT)	Price Year 3 (Excl VAT)	Price Year 4 (Excl VAT)
E2.1	Planning services	Per project	R 22 800,00	R 24 396,00	R 26 103,72	R 27 930,98
E2.2	Project management services	Per project	R 22 800,00	R 24 396,00	R 26 103,72	R 27 930,98
E3.3	Implementation services	Per project	R 120 000,00	R 128 400,00	R 137 388,00	R 147 005,16
						R 157 295,52

Labour costs – ad hoc							
E3	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)
E2.1	Project Manager	Per Hour	R 850,00	R 850,00	R 900,00	R 900,00	R 1 000,00
E2.2	Architect	Per Hour	R 950,00	R 950,00	R 1 000,00	R 1 000,00	R 1 050,00
E2.3	SME (Subject Matter Expert)	Per Hour	R 950,00	R 950,00	R 1 000,00	R 1 000,00	R 1 050,00

Service Level Agreement					
E4	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 5 (Excl VAT)
E4.1	As per relevant SLA	Included in managed services	Included in managed services	Included in managed services	Included in managed services

Managed Services			
E5	Services Description	Annual Rate (Rand) Year 1 (Excl VAT)	Annual Rate (Rand) Year 5 (Excl VAT)
		Annual Rate (Rand) Year 2 (Excl VAT)	Annual Rate (Rand) Year 4 (Excl VAT)

E5.1	Managed service to operate the Enterprise Data Loss Prevention platform 8 x 5 business hours only	R 720 000,00	R 770 400,00	R 824 328,00	R 882 030,00	R 943 773,00
------	---	--------------	--------------	--------------	--------------	--------------

Schedule H: Cloud Access Service Broker (CASB)

H1	CASB solution					
	Required Item / Description of Item	QTY	Part number	Supplier OEM Price (Excl. VAT)	Mark-up Percentage (%)	
H1.1	CASB solution for Office365 E3 access for 18000 users. Includes Exchange Online, SharePoint Online, Teams and OneDrive only.	18000	NSKP-PKG-SAAS-PROF	R 3 040 200,00	10 %	
H1.2	CASB solution for SAP Success Factors access for 18000 users	18000		R 0,00	10 %	
H1.3	CASB solution for Microsoft Azure access for 1000 users	1000		R 0,00	10 %	
H1.4	CASB solution for Amazon Web Services (AWS) access for 1000 users	1000		R 0,00	10 %	
H1.5	Support	1	NSKP-SUPPORT-PRE	R 550 800,00	10 %	

H2	Project Services						
	Services	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)
H2.1	Planning services	Per project	R 4 250,00	R 4 547	R 4 865	R 5 206	R 5 570
H2.2	Project management services	Per project	R 14 250,00	R 15 247	R 16 314	R 17 456	R 18 678
H2.3	Implementation services	Per project	R 38 000,00	R 40 660	R 43 506	R 46 551	R 49 810

H3	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)

H3.1	Project Manager	Per Hour	R 850,00	R 850,00	R 900,00	R 900,00	R 1 000,00
H3.2	Architect	Per Hour	R 950,00	R 950,00	R 1 000,00	R 1 000,00	R 1 050,00
H3.3	SME (Subject Matter Expert)	Per Hour	R 950,00	R 950,00	R 1 000,00	R 1 000,00	R 1 050,00

H4	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)	
H4.1	As per relevant SLA	R 25 000,00	R 26 750,00	R 28 622,00	R 30 626,00	R 0,00	
H5	Training						
	Required Item Description of Item	QTY	Part number	Supplier OEM Price (Excl. VAT)	Mark-up Percentage (%)	Final Price	
H5.1	Administrator	1	NSKP-TR-CST	R 79200	10 %	R 87 120	
H5.2	Advanced Administrator	1		Not Applicable	10 %	R 0	
E6	Training or equivalent						

	Required Item Description of Item	QTY	Part	Supplier OEM Price (Excl. VAT)	Mark-up Percentage (%)
E6.1	Administrator			R 17 293,61	10 %
E6.2	Advanced Administrator			R 0	10 %

A6 - 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.

Schedule B: Vulnerability Management – Background and Requirements

The City currently uses the Tenable.SC Vulnerability Management platform in order to perform extensive vulnerability assessments of the environment. It has now become necessary to further expand the reach of the system due to the City's IT security and compliance requirements.

The Tenable.SC web application scanner (WAS) currently does not meet the City's requirements from a reporting perspective, which impacts the City's ability to remediate detected vulnerabilities. Hence the reason for the City requesting additional bids for Web Application Scanner.

The vulnerability management tool(s) is required to perform vulnerability scans which conform to the CIS-certified (Centre for Internet Security) audit standards, in order to comply to the standards, set by the Auditor-General of South Africa for operating systems and databases. This requirement is mandatory.

The following environments are to be scanned for operating system, database and application vulnerabilities:

1. Windows Server 2012/2016/2019 and all variants
2. AIX 7.2
3. SUSE Linux 11, 12, 15
4. Red Hat Linux 7, 8
5. Microsoft SQL Server 2014/2016 and all variants
6. Oracle 11.2/12c and later
7. SAP HANA
8. IIS 7.5 and later
9. Apache 2.2 and 2.4

10. MySQL 5.3 and later
11. MariaDB 10 and later
12. SAP Portal
13. ESRI ArcGIS
14. Microsoft technologies
15. SAP technologies
16. Firewalls

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.

Functional 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.

#	Requirement / Question	Description / Technical Response
---	------------------------	----------------------------------

B 1	Describe in detail how to perform a vulnerability management scan on a host residing on the City's internal network. Active scans are scheduled by using a scan template, which provides target IPs, policy template, credentials and schedule selection. Schedules can be daily, weekly, monthly, dependent on other scans or manual. There is also a Blackout window feature which will prevent scan launches at specific times. Additionally, IPs can be blacklisted so they are never scanned. The default standard policy that would be obtained from using default policy values provides an ideal starting scan policy to scan a production environment. It is also possible to fully tailor scan policies to meet the specific requirements of the scan. Scan results offer detailed information on the top discovered vulnerabilities, and lists the affected hosts tracked within the Tenable product. Results also provide links that detail the steps to mitigate the risk of
-----	--

#	Requirement / Question	Description / Technical Response
		the vulnerabilities, including resources from CVE, BID, and vendor knowledgebase articles, where applicable. Additionally, the reported results indicate if the vulnerability is exploitable and by which exploit platform. All vulnerabilities detected by Tenable will include any applicable CVE references. Vulnerabilities can be filtered and searched based on the CVE.
B 2	Describe in detail how to make the results of the vulnerability management scanways. These are scheduled, on demand, available to the relevant team responsible for support and maintenance.	All reports can be run in several different ways. These are scheduled, on demand, attached to an alert, and as part of the scanning process. These reports can be distributed to end users via email, reporting sites such as SharePoint, and exported via the API.
B 3	What options would you recommend to configure when scanning a new Windows Server 2012 R2 server that has just been deployed, and is about to go into production?	An authenticated scan against the server could be used to reveal any missing patches or other vulnerabilities. Furthermore, an audit can be attached to the scan, which would report on the server's compliance to a set of technical controls. Tenable provide audits for industry standard best practice guidelines, such as CIS, DISA STIG, NIST SCAP, as well as recommended vendor settings. These audits can be edited to fit local requirements or created to match a customer's bespoke requirements. Measuring patch and compliance level before rolling out the server to production
#	Requirement / Question	Description / Technical Response

		will mitigate any new threats being introduced to the environment. Note that Tenable solutions perform "intelligent" scans, meaning one scan template can be applied to any system, regardless of platform, OS, device type. The scans will only apply tests that are relevant to each individual target.
B 4	When options would you recommend when configuring a web application scan for an externally facing web server hosted on a SharePoint front end server that contains personal information?	Tenable.sc should be used to scan the SharePoint front end server in the manner described in response B3 Tenable.io Web Application Security (WAS) should be used to scan the web application on the server. Tenable.io WAS offers significant improvements over the existing Web Application Tests policy template provided by the Nessus scanner, which is incompatible with modern web applications that rely on Javascript and are built on HTML5. Tenable.io WAS provides comprehensive vulnerability scanning for modern web applications. Accurate vulnerability coverage minimizes false positives and false negatives, ensuring that security teams understand the true security risks in their web applications. The product offers safe external scanning that ensures production

#	Requirement / Question	Description / Technical Response
		web applications are not disrupted or delayed, including those built using HTML5 and AJAX frameworks. Tenable WAS allows site overview scans, which do not require authentication. These help to get a general understanding of the content reviewed in the full scan. Site overview scans also attempt to potentially required authentication, including login forms and HTTP authentication. Standard web application scans perform a series of tests against the site to look for OWASP Top 10 vulnerabilities.
B 5	As availability of web services are critically important, how would you recommend the balance between availability and security is maintained?	Tenable.io Web Application Scanning is a Dynamic Application Security Testing tool, and does not scan code. Best practices would be to use a SAST tool very early on in the SDLC in addition to a DAST tool later in the SDLC, before pushing any application into production. The Tenable.io cloud service strives to provide a 99.95% or better uptime, and have delivered 100% uptime on the majority of services. Tenable.io makes extensive use of the AWS platform and other leading technologies to ensure that our customers experience the best possible service and overall quality.

#	Requirement / Question	Description / Technical Response
B 6	When performing a database vulnerability assessment, what is the overhead to both the application and database servers?	Actual scan performance will be dependent on numerous factors and dependent on local variable, such as the type of database, if credentials are used, etc. Tenable.sc has a number of self-tuning techniques to improve overall scanning performance. In addition, Tenable.sc provides multiple configuration options in order to throttle scan performance and minimise impact to the network and endpoints. These configurations include number of hosts that are tested at any one time during a scan and the number of checks performed on each host at any one time. Furthermore Tenable.sc supports different scanning methodologies that also reduce any possible impact.
B 7	Describe the different types of database assessments that can be performed, and the benefits of each one.	Tenable Products can audit databases for security and configurations settings, discovery supporting many common and uncommon 3rd party applications and databases. We support credentials for Databases (DB2, Informix/DRDA, SQL Server, MySQL, Oracle, PostgreSQL and MongoDB), ADSI, IBM iSeries, RHEV, PAN-OS, VMware SOAP API, and X.509}.

#	Requirement / Question	Description / Technical Response
B 8	Describe how to ensure secure authentication is used, for both DBAs and users.	Tenable.sc provides the following authenticated methods for performing credentialed scans and configuration audits: Windows Operating Systems - CyberArk Vault - Kerberos - LM Hash - NTLM Hash - Password - Thycotic Secret Server SSH Authentication for unix, network device and other systems: - Certificate - CyberArk Vault - Kerberos - Password - Public Key - Thycotic Secret Server Databases: - Microsoft SQL - DB2 - Informix/DRDA - MySQL - Oracle - PostgreSQL Tenable.sc has integrated with leading credential management providers, CyberARK and Thycotic, to enable seamless authentication for scanned hosts, ensuring

#	Requirement / Question	Description / Technical Response
		optimal scan coverage while making it simpler for users to configure. Managed credentials are added to scans identically to a standard remote credential and are currently available for Windows authentication. With direct access to the target operating system, the solution has the ability to perform checks not possible through a credentialed scan, not limited to but including the following: - Exact patch state of the operating system and installed software - Audit of all configuration settings - Current open ports through netstat - Running malware checks - Threat correlation against the host's IP address (if public) -Threat correlation of then present communication via netstat results
B 9	The critical databases that are currently assessed are Oracle. One of the applications is currently being redeveloped onto a .Net 4.7 platform, with a MS SQL 2014 DBMS. Describe the impact of this change to the vulnerability management scan, report and licensing.	This should have little impact on the scan itself. The new credentials would need to be added and then the same scan settings can be used, as described in B3. Reporting may need to be adjusted to make sure the new database is included in the report scope.

#	Requirement / Question	Description / Technical Response
		There would be no impact on licensing
B 10	What options would you recommend to configure when scanning a new AIX or Linux server that has just been deployed, and is about to go into production?	An authenticated scan against the server could be used to reveal any missing patches or other vulnerabilities. Furthermore, an audit can be attached to the scan, which would report on the server's compliance to a set of technical controls. Tenable provide audits for industry standard best practice guidelines, such as CIS, DISA STIG, NIST SCAP, as well as recommended vendor settings. These audits can be edited to fit local requirements, or created to match a customer's bespoke requirements. Measuring patch and compliance level before rolling out the server to production will mitigate any new threats being introduced to the environment. Note that Tenable solutions perform "Intelligent" scans, meaning one scan template can be applied to any system, regardless of platform, OS, device type. The scans will only apply tests that are relevant to each individual target.

#	Requirement / Question	Description / Technical Response
B 11	What options would you recommend to configure when scanning an existing Extreme Networks S8 core switch that has just been updated with the latest available firmware, to confirm that the device has been securely configured as per standard operating procedures.	Tenable.sc can be used to audit ExtremeXOS. The ExtremeXOS audit includes checks for the password policy, banner configuration, inactivity timeout setting, logging & audit settings, insecure services, device license information, and SNMP settings.
B 12	The City of Cape Town is required to ensure compliance with relevant security standards to ensure confidentiality, integrity and availability of information. Against what standards will the proposed vulnerability management solution be able to assess the City's ICT environment against? Describe in detail how this will assist the City to maintain and indicate its security posture when audited, whether externally or internally.	Managing Governance, Risk Management, and Compliance (GRC) grows more complex with each newly developed set of regulations or standards. Tenable.sc has the ability to monitor configuration compliance with a variety of standards including CIS, HIPAA, to assess the City's ICT environment NIST 800-53, PCI DSS, and DoD 8500.2. This dashboard shows the security manager a summary of compliance checks security posture when audited, supported by Tenable.sc. Using Tenable's products to perform vulnerability scans and compliance audits allow users to obtain all of necessary data in a single instance. If you know how a server is configured, how it is patched, and what vulnerabilities are present, you can determine measures to mitigate risk. At a higher level, if you aggregate this data for an entire network or asset class, you can analyse

#	Requirement / Question	Description / Technical Response
		security and risk globally. This allows auditors and network managers to spot trends in non-compliant systems and adjust controls to fix these on a larger scale. Tenable.sc's various compliance and standards based configuration audit templates include, but not limited to: COBIT controls, CERT recommendations, CIS best practice guides, DISA STIGs, GLBA guidelines, HIPAA profiles, NIST SCAP and FDCC content, ISO 27002/17799 Security Standards, NSA best practice guides, ITIL codes of practice, PCIDSS configuration and hardening requirements, SOP, Recommended vendor settings, SOX, USGCB, MSCM, FISMA, OWASP. Performing a compliance audit scan is not the same as performing a vulnerability scan, although there can be some overlap. A compliance audit determines if a system is configured in accordance with an established policy. A vulnerability scan determines if the system is open to known vulnerabilities. Organizations can deploy and customize audit files to meet their local security policy. Once the audit file is customized, the file can be used with Tenable.sc to manage and automate the configuration compliance process.

#	Requirement / Question	Description / Technical Response
B 13	Provide examples of reports which highlight detected vulnerabilities. Also, include how these reports provide relevant information to remediate or work around detected vulnerabilities.	Tenable.sc offers over 400 templates and the list keeps growing, all of which are available out of the box at no additional charge. Templates can be customized in addition to providing a flexible template library for new and customized template versions. Nearly all reports provide an executive summary then pages with detail. Tenable's remediation report provides detailed information on the top discovered vulnerabilities, and lists the affected hosts tracked within Tenable.sc. This report also contains steps to mitigate the risk of the vulnerabilities, including resources from CVE, BID, and vendor knowledge base articles. Additionally, this report indicates if the vulnerability is exploitable and by which exploit platform. The report includes executive summary, active vulnerability remediation plan, passive vulnerability remediation plan, and a compliance check remediation plan. Approved users can run remediation scans to verify vulnerabilities have been addressed correctly. An example of this report can be viewed at: https://www.tenable.com/sc-report-templates/remediation-instructions-report-by-vulnerability

#	Requirement / Question	Description / Technical Response
14	Describe in detail how the console or system may be configured to detect and escalate any vulnerabilities, which have not been accepted, which have been present for more than three months, in contravention of policy.	Scans are automated and completed on a regular basis. Tenable discovers, assesses, and reports on certificates being utilized on host systems as a component of the scan process. This is accomplished by utilizing one or several of the plugins that are associated with Certificate discovery and assessment. These plugins report on validity, aging, cypher strength, as well as additional items. Tenable supports secure shell (ssh) with the ability to escalate privileges for vulnerability scans and configuration audits on Unix systems. Tenable also provides a manual workflow to accept or recast risk of vulnerabilities. Tenable can define exceptions to vulnerabilities that cannot be fixed. This is done through the "Accept Risk" button. Accepting a risk means that the vulnerability will not be reported. A comment field is available to document why the risk is being accepted. Accepting a risk can be done for a single IP address, a group of assets, or all assets. Accepting a risk can be done permanently, or an expiry date can be set for the acceptance, after which the vulnerability will appear in reports again. All accepted risks can be reviewed for auditing purposes. Tenable can define exceptions for just a particular IP address, an asset group,

#	Requirement / Question	Description / Technical Response
		or for all assets. Tenable can also provide an expiry date for accepted vulnerabilities, at which time the vulnerability will show in the reports again. All accepted risks have a comment field to state the reason for the exception. When a risk has been accepted, the vulnerability no longer shows in any dashboards or reports.
B 15	Describe in detail how the system may be configured to provide detailed technical reports for administrators, departmental reports per department for managers to ensure relevant and applicable management reporting to ensure management control, and overview for Governance and Security teams.	Tenable.sc asset classification enables systems to be tagged as belonging to customer-defined groups e.g. the internal network, external network and DMZ assets can all be tagged as part of the "Network structure" group, or MySQL, MSSQL and Oracle assets can be tagged as part of the "Databases" group. Once defined the asset tagging can be used throughout Tenable.sc's interface for use in analysis, reporting, alerting, dashboarding, user profile restrictions, scanning, ticketing, risk recasting and more. Once asset tagging has been defined, a user's role can also be configured to restrict their view of the data and scanning scope, data repository access, filterable assets, scanning credentials, queries and scan policies, etc.

#	Requirement / Question	Description / Technical Response
B 16	How would the vulnerability management system integrate with the existing McAfee SIEM solution	There are two ways we work with SIEMs. First, Tenable's products send via the export of syslog files via alert workflow process. For NERC CIP, actions and activities within the Tenable tool will be logged and then can be monitored by your SIEM. Second, we can integrate with SIEMs via our RESTful API. It is published and offered at no additional fees. RESTful APIs are for developers who want to integrate Tenable's products with other standalone or web applications, and administrators who want to script interactions with the Tenable management console. We have pre-built SIEM integrations with IBM Tivoli Endpoint Manager, IBM's QRadar SIEM, and Splunk. Tenable.sc is able to send data out to McAfee ePO via a pre-built integration, so that these solutions can use the vulnerability data to correlate with SIEM events or antivirus events.

B 17	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.	Attached with this response is detailed document depicting our technical support plans. In summary: Advanced Technical Support is available at no fee to our subscription customers using our enterprise products. Our Support Plan has an aggressive Response Time Objective
-------------	--	--

Schedule E: Data Loss Prevention

Background and Requirements

The City of Cape Town intends to implement a Data Loss Prevention (DLP) solution as a new initiative in line with the POPI Act (POPIA) to address unintentional or intentional disclosure of confidential data, personal information and intellectual property.

The proposed DLP solution should be an enterprise content-aware solution that covers all endpoints such as servers, desktops, laptops and mobile devices, as well the web and email gateways. The DLP solution should also integrate with cloud hosted environments, outside of the City's control, such as Gmail, Dropbox, Google Drive, Skydrive, Office365, etc.

The solution must also provide a centralised management console for monitoring and management across the various environments.

Given the above, the proposed DLP solution shall have the following minimum features:

- a) Identify confidential data, personal information and intellectual property.
- b) Identify data leakage of confidential data, personal information and intellectual property
- c) Protect confidential data, personal information and intellectual property by enforcing security controls
- d) Include both on premise and Cloud environments
- e) In the case of a potential infringement, the solution must allow the users line manager to authorise the release of an email containing potential sensitive information, without referral to the City's IT Security team, but with the necessary audit trails to ensure accountability
- f) Monitor user actions to understand the risk involved

g) Ease of use for users

The enterprise DLP solution is required to integrate into the existing ICT infrastructure:

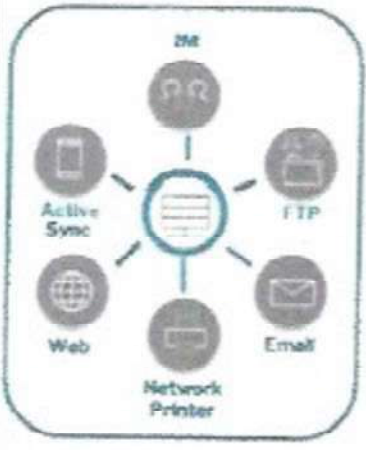
- Microsoft Active Directory
- Extreme Networks S6 & 8 switches
- Citrix ADC reverse proxy
- Microsoft Systems Centre Operations Manager
- pSense proxy servers
- Trend Micro anti-malware
- Trend Micro Deep Discovery Analyser
- Trend Micro Deep Discovery Email Inspector
- Trend Micro Deep Discovery Web Inspector
- Microsoft Internet Information Services web servers
- Apache web servers
- Windows 2012 R2 Server
- Windows 10 x64 Professional and Enterprise
- AIX 7.2
- SUSE Linux
- VPN – Palo Alto
- Tenable.SC Vulnerability Manager
- Oracle databases
- SAP HANA databases
- SQL databases
- MySQL databases
- MariaDB databases
- Extreme Networks Wireless Controllers
- SAP
- Trend Micro Hosted Email Services Cloud

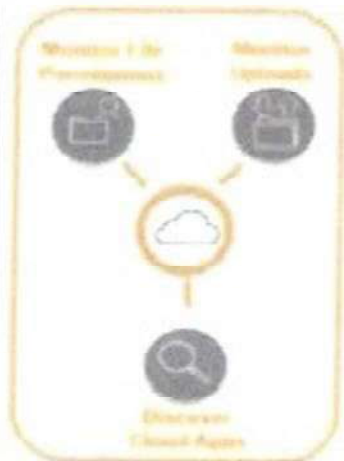
Functional Questions

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
		Forcepoint DLP, as mentioned above, is controlled via the DLP Manager Server, which configures up to 200 modules to enforce a centralized policy in a complex and distributed working environment. DLP capabilities is divided into two categories: Regulatory Compliance data and Customer custom data. In the below subsections not that these control points will focus on both Regulatory Compliance as well as Custom data. Data at Rest: Data at Rest Fingerprinting has two tasks: a) learn what Customer's custom data looks like by means of hash fingerprinting. Secondly scanning (Forcepoint calls this "Crawling") databases and File Shares to finds sensitive data (Reg Compliance or Customer). The Forcepoint Endpoint has the ability to look for both Custom as well as Regulatory Compliance data too on its local HDD where it is installed onto. Lastly, the DLP Cloud Applications module will scan data at rest inside Office365 using the same Customer and Regulatory data fingerprints too. The Crawler server has an in-built Optical

#	Technical Requirements / Questions	Description / Technical Response
		Character Recognition (OCR) service to scan images at rest for sensitive data. This OCR capability can be performed on File Stores.  Data in Motion: Forcepoint Protectors are Linux-based systems that will monitor HTTP, HTTPS*, SMTP, FTP and IM channels for data leaks in the network (movements between systems on LANs\WANs). DLP Protectors will report into the DLP Manager, and Monitor/Block as required. If the City of Cape Town (CoCT) is using MS ActiveSync, then the DLP Protector can be used there too to monitor this channel. It will be installed inline into the ActiveSync traffic stream. In this setup the DLP Protector is now called a DLP Mobile Agent. The DLP Crawler can also be an OCR Service. A OCR Server can be attached onto a DLP Protector to monitor data leakage within images

#	Technical Requirements / Questions	Description / Technical Response
		sent across the network and instruct the DLP protector to block based on its analysis.  The diagram illustrates a central hub (represented by a circle with horizontal lines) connected to six data leak channels, each represented by an icon and a label: IM (Instant Messaging), Active Sync, Web, Network Printer, Email, and FTP. The connections are shown as lines radiating from the central hub to each channel icon. Data in Use: The Forcepoint Endpoint Agent can be installed onto Windows and Mac Computers. The DLP Endpoint Agent can perform block, monitor, and pop-up message actions for data leak channels that it looks after. In addition to this it can encrypt sensitive data that move sot the External HOD/USB channel. Things such as the Clipboard is monitored for copy/paste actions. Also, plug-ins into Browsers and Outlook is there to monitor traffic on those applications. The DLP Endpoint Agent will act upon DLP Policies wall the time, irrespective if it is on, or off of the network.

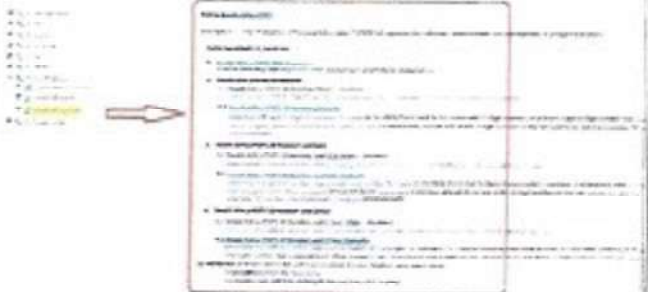
#	Technical Requirements / Questions	Description / Technical Response
		 DLP Cloud Applications module: A note about this: as discussed above DLP Cloud apps extends data controls into the Cloud. Now up/downloads can be monitored and reported on. DLP Cloud Applications also can unshare sensitive data that has been shared externally, internally, or both. 

#	Technical Requirements / Questions	Description / Technical Response
E 2	Describe in detail the capacity planning involved in order to ensure a scalable and stable working solution. Please include all infrastructure required to make the DLP solution work. Highlight any dependencies and integration required.	One Forcepoint DLP Manager will control the whole DLP Infrastructure. Server specs for the whole Forcepoint DLP ecosystem can be found here. DLP capacity depends on each Customer and their flows. For most part a baseline can be put forward to start off the DLP deployment, and we can scale more and more servers as the City of Cape Town evolves in its IT transformation journey. Note: The DLP Supplementary Sever as per the server specification link in the paragraph above) is the same sever used for DLP Crawling, DLP Endpoint Server, and OCR Server capabilities. The DLP Crawlers can scan approx. 240GB/day and this is a baseline to decide how many DLP Crawlers would be required in order to scan the required DBs and File Storage areas that CoCT possess. In addition, DLP Crawlers should always be placed as close to their data stores as possible to speed up scanning of the file server/database. DLP Endpoint Servers are the middleman between the DLP Endpoint Agents (deployed to the CoCT Userbase) and the Forcepoint DLP Manager server. The soft-limit rule is to connect a large amount of DLP Endpoint

#	Technical Requirements / Questions	Description / Technical Response
		Agents to one DLP Endpoint Server. So regional DLP Endpoint Servers should be placed in large remote sites. The soft-limit ratio of DLP Endpoint Servers to Endpoint Agents is 5,000 Endpoints to one Endpoint Server. A Backup DLP Endpoint Server can be a remote server to where the User works from, and this can be architected as required. Email Channel: As mentioned above the DLP Protector can be placed inline in MTA mode to inspect email leaving the organisation. MX costing or a Network Load Balancer (NLB) can be used to load balance between DLP Protectors. As SMTP traffic increased, DLP Protector servers can be added to the array to counter this. OCR Servers can be attached to the DLP Protectors in a 1:1 ratio. Requirements will have to be specified after technical sessions are conducted with CoCT. HTTP/HTTPS/FTP/IM Channel: Any CoCT device that can monitor these channels can use the DLP Protector assuming /CAP capability is in possible from that service. HTTPS traffic can also be interrogated from the DLP Protector as long and the third- party system can perform HTTPS decryption/inspection. Network Load Balancer (NLB) can be used to load balance between DLP Protectors in this state. As the servers require, more DLP Protectors can scale as required. OCR Servers can be attached to the DLP Protectors in

#	Technical Requirements / Questions	Description / Technical Response
		a 1:1 ratio. Requirements will have to be spec'ed after technical sessions are conducted with CoCT. DLP Endpoint Agent: a DLP Endpoint Agent will be installed onto each Windows and Mac Endpoint. DLP Analytic Engine Server: The DLP Analytics Engine Server is used to monitor the logs coming into the DLP Manager and the show an Incident Risk Ranking per User who has DLP incidents on the system. One DLP Analytic Engine Server per deployment is required. SOL Server: The Forcepoint DLP System uses SQL as its database as required. Forcepoint recommends a SOL Server with a storage area of 750GB to start off with. File storage: The Forcepoint DLP incidents are stored onto a SAMBA file share of your choice. The amount of storage depends on the amount of DLP incidents generated and caught by the system. Forcepoint recommends a 3Tb storage area to start off with.

#	Technical Requirements / Questions	Description / Technical Response
E 3	Describe the endpoint operating systems supported and the capabilities of each.	The Forcepoint Endpoint has a support matrix of Operating Systems and can be viewed here. The DLP Endpoint Agent can Monitor, Block and Confirm across all these data channels below *In addition to the three above mentioned actions the DLP Endpoint Agent can encrypt on the USB channel too: Endpoint Channels Email: Permit ▼ Application control: Block ▼ Removable media: Encrypt with profile 123 ▼ HTTP/HTTPS: Permit ▼ LAN: Confirm ▼ Printing: Permit ▼
E 4	Does the DLP offering provide the capability to monitor social media, Web and cloud storage interactions? If yes, provide details of these capabilities.	The Forcepoint DLP system has agents set out across the CoCT ecosystem in order to monitor for DLP threats. The DLP Protectors mentioned above can integrate with the Web system via ICAP capabilities. This is especially useful if the third-party can provide for HTTPS Inspection/SSL Decryption. In this case HTTPS traffic can be inspected by Forcepoint DLP Protectors as well. Therefore, any cloud storage transactions that can be monitored by the DLP Protectors will show value to the CoCT. DLP Cloud Apps is a capability to extend DLP controls into the Cloud space and monitor the likes of Office365 (SharePoint online and

#	Technical Requirements / Questions	Description / Technical Response
		OneDrive), G-Suite, Salesforce, Box, Dropbox for Business as well as ServiceNow. In this case any Up/Download actions will be monitored. In addition to this DLP Cloud Apps will remove sharing if data is shared externally, internally, or both. Lastly recall that DLP Cloud Apps can scan for data at rest on the 6 above-mentioned application.
E5	Please explain how the proposed DLP solution will safeguard confidential data and ensure compliance across the different environments.	As mentioned in E1 above Forcepoint has the capability to monitor Data at Rest, In Motion, and in Use. Having Forcepoint connected with Agents in channels such as Email, Web and Endpoint offered "eyes" at critical places within the organisation. Having Forcepoint's central management system means that all these Agents can feed back to a central control point. This proved uniformity across the DLP ecosystem because configuration, logging, as well as DLP incidents all come back to that central point. In this way you provide for compliancy across the different environments (channels) of data leaks. Example:  Predefine DLP Policies looking for PDI information...

#	Technical Requirements / Questions	Description / Technical Response
		 With one place to control the action (Block/Monitor/Confirm) across the multiple data leak channels makes it simply and easier to manage...
E 6	Highlight the differentiating characteristics and features that distinguish your product from other DLP solutions.	Drip DLP: Data theft where confidential information is exported in low volumes per request (drips) to avoid detection over a defined period of time should also be considered. Forensic reporting that shows what data was blocked by data-theft defences from leaving an organization completes the picture. Integration with Data Labelling solutions: Forcepoint can integrate with Microsoft AIP, TITUS as well as Boldon James at no extra licensing cost. This integration now gives the CoCT the ability to have Forcepoint DLP correct data labels labelled incorreced whenever the DLP Endpoint: a) performs a Data at Rest scan on the

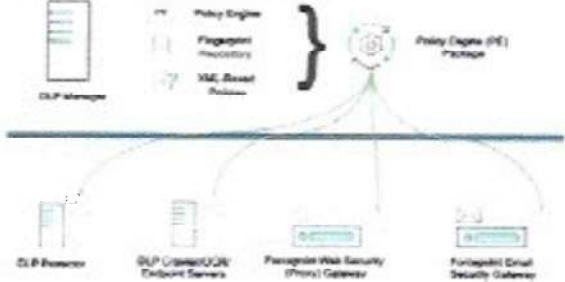
#	Technical Requirements / Questions	Description / Technical Response
		Endpoint Agent, and b) When Users move data across the Endpoint. OCR capabilities: As mentioned in E1 and E2 above the ability for our product to use OCR to find Images when performing scans of Data at Rest and well as Data in Motion offers that additional layer of protection of sensitive data. This included Office Documents and PDFs. Largest global Compliance Classifier library: Forcepoint has the largest library comprising of PreciseID fingerprinting and Machine Learning to protect sensitive data. Flexible policy framework to address Customer Use Cases. Policy Management: One Management station to control Data at Rest Discovery, Data in Motion, Data in Use as well as extension into Cloud for Data in motion and data at rest capabilities. As your data moves to the cloud so does the DLP policy with it. Customers who enjoy our DLP Suite as well as CASB Security Suite will have the ultimate DLP controls, where data moving in the CASB system will be blocked in Real-time.
E 7	Describe in detail the features and configuration options for the centralized (single) management console across environments	As mentioned on E1 the Forcepoint DLP system will offer Data at Rest, Data in Motion, as well as Data in Use capabilities. This helps to control the data in strategic locations within your electronic ecosystem. Forcepoint DLP offers a myriad of capabilities to

#	Technical Requirements / Questions	Description / Technical Response
		best understand what sensitive data may look like to you as our Customer: Once we understand what it is that you wish to protect then it is a matter of creating the required DLP policies and rules: Predefine DLP Policies... Editing the Action Plan section, you can choose your desired outcome With one place to control the action (Block/Monitor/Confirm) across the multiple data

#	Technical Requirements / Questions	Description / Technical Response
		leak channels make it simply and easier to manage... Writing the DLP ruleset following the Who What Where How -> Action methodology:  Because all the DLP Agents dotted across your organisation registers with the DLP manager, the DLP manager will push our new configuration where required...and get reports back from these Agents as sensitive data passes through them.  This screen above shows some of the components/Agents that can be registered to the DLP manager:

#	Technical Requirements / Questions	Description / Technical Response
		1. "Forcepoint DLP Server": The DLP manager itself. 2. "Forcepoint DLP Server on ENDPOINT-SERVER": Example of a Server used as an Endpoint Server to a set of DLP Endpoint Agents. The DLP Endpoint Agents are configured to speak with the Endpoint Server who in turn will speak with the DLP Manager Server. Spin as many as is required for your deployment strategy. *Deep technical design will need to take place to determine the requirement here*. 3. "Forcepoint DLP Server on OCR-SERVER": Example of a Server used for Crawling and/or OCR capabilities. Spin as many as is required for your deployment strategy. *Deep technical design will need to take place to determine the requirement here*. 4. "Protector on protector25587": A DLP protector Server. Used for SMTP, HTTP, HTTPS, FTP, IM and ActiveSync communication inspection. *Note: the ActiveSync DLP Protector will be called Mobile Agent*. *Deep technical design will need to take place to determine the requirement here*. 5. "Forcepoint Content Gateway server on webwgc.demo.com": an example of a Forcepoint Web Security (Proxy) Gateway with full built-in DLP Engine. *Not part of this DLP RFP response.* "Forcepoint Email Security Gateway server on email-wgc.demo.com": an example of a

#	Technical Requirements / Questions	Description / Technical Response
		Forcepoint Email Security Gateway with full built-in DLP Engine. *Not part of this DLP RFP response. *
E 8	Describe in detail the features and configuration options for the policy engine.	The Policy Engine is the Forcepoint DLP component responsible for all data analysis and policy enforcement.  <pre> graph LR INPUT[INPUT Data and Metadata to Analyze] --> PE[Policy Engine] PE --> OUTPUT[OUTPUT Detailed Incident] </pre> The policy engine is responsible for parsing your data and using analytics to compare it to the rules in your policies. You can have multiple policy engines in your Data Security system to manage high transaction volumes. - There is always a policy engine on the DLP Manager and DLP Protectors (including Mobile Agent Servers). - The Policy engine is allow coped to the DLP Servers offering the following capabilities: - o DLP Crawling capabilities - o Endpoint server capabilities - o OCR Servers. - If you were to invest in either the Forcepoint Web Security (Proxy) Gateway as well as the Forcepoint Email Security Gateway then a full DLP engine (with Policy Engine)

#	Technical Requirements / Questions	Description / Technical Response
		would reside on these respective platforms too. - The DLP Endpoint Agent has a modified version of the Policy Engine which allows for a smaller footprint.  This shows the makeup of the Policy Engine (PE) Package. The PE package is pushed to all DLP infrastructure that houses the copy of the PE Package.
E 9	Explain how the DLP solution supports dynamic application of a policy setting based on the analysis of content.	One of Forcepoint's greatest strengths is Drip DLP, reference above in E6. Image setting up a DLP Policy looking for certain data - say - POPI. We expect a threshold of- say - 3 pieces of POPI information per transaction to move via our Network DLP systems before we will block it. This means that a transaction where 2 or less pieces of POPI information is passed through out system we would not block, nor record it. Forcepoint's Drip DLP constantly looks for data and records all transmissions of the data leaving via monitored DLP Channels irrespective of what the DLP policies state. Now, Forcepoint DLP will be able to catch a

#	Technical Requirements / Questions	Description / Technical Response
		person attempting to "siphon data out using a means of transmitting less than 3 POPI pieces of data per transaction Here is an example explanation: In the above example we have set a threshold of 3 or more entries of POPI data to be present in a single transaction in order to enforce a block. 1. If a User sends one POPI piece of data across the Endpoint Email channel, for example, the DLP system allows this...but we start a counter. 2. Now, if the same user (within the configured timeframe) now attempts to print a second piece of POPI data on a printer, the counter counts two pieces of POPI information. The printer job does run. 3. Now -when the User now attempts to post a third piece of POPI information via the HTTP channel, within the same time period as configured by the DLP Administrator, the counter now counts three pieces of POPI information leaked across a set of DLP Channels. The DLP channels utilised is not a factor in Drip DLP, but rather the Content (Data). Because the threshold of 3 was hit within the configured time period the User's attempt to leak the third piece of POPI information is stopped...together with any subsequent data leaks of POPI information within the set time period.

#	Technical Requirements / Questions	Description / Technical Response
E 10	Explain in detail the monitoring and reporting capabilities within the DLP solution	As mentioned above in E2 the DLP Manager is the central control point for DLP configuration, Logging as well as DLP incidents. This is a critical piece of the DLP ecosystem. The DLP Manager has a vast set of reports that can be run by the required DLP Administrators. These predefined reports can also be duplicated and customised to fit your requirements. Lastly Role Based Access Control (RBAC) can set who may be allowed Reporting privileges and who may not. The full range of reports: •  Recent reports •  Incidents (last 3 days) •  Incidents (last 7 days) •  DLP Dashboard (last 7 days) •  Top Violated Policies (last 7 days) •  All Violations by Severity and Action (last 7 days) •  Top Sources and Destinations (last 7 days) •  Incident Trends (current quarter) •  Incident Status (last 7 days) •  Incidents List •  Incidents (last 3 days) •  Incidents (last 7 days) •  Incidents (last 30 days) •  Incidents by Severity (last 7 days)

#	Technical Requirements / Questions	Description / Technical Response
		• Risk Assessment • Top Violated Policies (last 7 days) • Top Violated Policies - Links to Removable Devices (last 7 days) • User Risk Summary (Data Theft Risk Indicators) • User Risk Summary (All Incidents) • Security Analysis • Incident Risk Ranking - Top Cases • My Incident Risk Ranking Cases • Severity and Action • All Violations by Severity and Action (last 7 days) • Credit Card Violations by Severity and Action (last 7 days) • PI Violations by Severity and Action • Sources and Destinations • Top Sources and Destinations (last 7 days) • Top Sources and Destinations - Credit Card Number Violations (last 7 days) • Top Sources and Destinations - PI Violations (last 7 days) • Top Sources and Destinations - PCI Violations (last 7 days) • Detective Dashboard • DLP Dashboard (last 7 days) • DLP Dashboard (current quarter) • DLP Dashboard (previous quarter) • Status • Incident Status (last 7 days) • Trends • Incident Trends (current quarter) • Incident Trends (previous quarter) • Geographical Location • WED DLP - Destination by Severity (last 7 days)
E 11	Describe in detail the detection techniques of the DLP solution that will discover and correlate data patterns?	Two major components which Forcepoint DLP believes will help uncover advanced DLP and risk technics are the Drip DLP function and the DLP Incident Risk Ranking capability. Drip DLP was explained in E9 above. Forcepoint DLP Incident Risk Ranking (IRR): How IRR works: The Analytics Engine is the brain behind the risk based data modelling. It's designed to deliver a holistic view of risk across multiple data loss channels and from all endpoint, gateway and cloud components. It can be deployed on virtual or physical hardware and can even work on a single data set, such as endpoint or email incidents. The Analytics Engine is included in all

#	Technical Requirements / Questions	Description / Technical Response
		Forcepoint DLP licenses free of charge. Incident Risk Ranking uses statistical data modelling and behavioural baselines to automatically identify and group incidents into cases. Each case is given a risk score 0-10, with 10 posing the highest risk to your organization. Data Loss Prevention - Incident Risk Ranking Incident Risk Ranking - Top Cases (previous 24 hours) 10  Incident Risk Ranking - Top Cases (last 7 days) 10  There is a five-step process involved in building the Incident Risk Ranking report 1. Related incidents form an activity chain of events and are then automatically grouped into cases. 2. A set of Bayesian data models classifies the activity-e.g., data theft-a broken business process or personal communication. 3. The system maintains both organizational and individual behavioural baselines to detect

#	Technical Requirements / Questions	Description / Technical Response
		anomalous activity within each data set. 4. A risk score is calculated for each case by combining the results of the data models with the behavioural baseline analysis. 5. The results are formatted and presented to the security operations team in the IRR report. 
E 12	How long does a typical installation of your DLP solution take for this size and complexity organisation?	A DLP Project is mostly driven by Business. The IT portion of the project is reasonably simple. Dependencies: Dependencies will need to be seeped out and prepared before installation of the DLP ecosystem within the CoCT. 1. These dependencies will include VMware environments in strategic locations across your organisation. Once that is done then Windows OS will be deployed onto these virtual hardware server allocations. Alt. option for physical servers are also fully supported. Here are the system requirements link.

#	Technical Requirements / Questions	Description / Technical Response
		2. Firewall rules to allow for inter-DLP-Ecosystem flows will then be allowed. 3. Change Control will be factored in to comply with CAB requirements. 4. AD Account right and the likes will be discussed and distributed to CoCT personal. 5. SQL Server requirements will be asked. 6. SAN/Storage will be required in order to house the SQL DB as well as the DLP Incidents (the forensic DB) onto: 750GB of SQL Storage and 3TB of SAN/SAMBA storage for the DLP Forensic DB. Forcepoint deployment stages: 1. The deployment of the DLP Manager and relevant Agents could take two- three weeks to complete. 2. The DLP SMTP Protector array will be brought in-line with the Email flow within the CoCT *Change Control required*. 3. The HTTP/S, FTP, IM DLP Protector array will be brought into play within the CoCT environment *Change Control required* 4. The DLP Manger and DLP Protector system will be brought into Monitor-only mode. Initial DLP basic functionality testing can take place for 1 week. 5. DLP Crawler servers will be linked to the DLP Manager and respective basic functionality testing will start. The testing can continue for 1 week. 6. Creation of DLP Endpoint Agent packs will be done and distributed to a

#	Technical Requirements / Questions	Description / Technical Response
		handful of testing machines. This will be done to confirm stability of the DLP Endpoint Agent across the CoCT desktop/laptop builds. Initial testing can be done for 1 week. 7. Distribution of the DLP Endpoint Agent will start via CoCT third-party distribution tool. Timeframe is unknown and dependant on the third-party software package distribution tool. 8. For a period as required interviews with the Business Heads will take place so that they can get an understanding of the DLP project, what can be achieved, and what information would be required from these Business Heads. The type of information can include: a) what data is important to them? b) Who within their section(s) will monitor/review DLP leaks? c). What action would they like done in DLP leaks? 9. A series of testing will commence with each Business Section as the DLP policies are laid down and tested. Length of time is all dependant of the data received from the sections as well as the complexity of their DLP respective asks. 10. *Optional* DLP can be integrated into Boldon James or Microsoft AIP to bolster the value of the Data Labelling project within CoCT. In time the system will mature from a "Monitoronly" system to a "Notify/Prompt" system to a full "Block" system (on DLP Policies where Blocking mode is required). During this time adjustment will take place to the DLP Policies as the Userbase

#	Technical Requirements / Questions	Description / Technical Response
		started to understand this new Business Process/Adoption within the organisation. During the DLP Deployment Stages Skills transferred should be done so as to bring the FTEs up to speed with the technology that they will be looking after.
E 13	In your experience once the DLP solution has been successfully deployed to all environments, how many full time employees are required to optimally support and maintain the system? What skills are required to perform these functions?	Two FTEs should be deployed in a global DLP Administrator role. These individuals will have to maintain the health of the DLP system, perform migrations/upgrades, and assist with DLP Policy creation/maintenance as required. These FTEs should have a keen understanding of DLP and IT. They will be employed into the IT Section/cost centre and thus managed the technical aspect of the solution. Then, typically, each Business Head/Section will have a group of Data Analysers to look after the DLP breaches/incidents generated within their respective sections/departments. These personal will not look at the IT aspect of the system but, rather the DLP Polies for their respective section and the DLP incidents generated by personal working within their Business Section. These Data Analysers should be trusted personal within the respective Business Sections. These Data Analysers should also have the correct

#	Technical Requirements / Questions	Description / Technical Response
		clearance levels to view sensitive data and personal tracking. This is necessary considering that they will be required to view each DLP incident and report/take action as required.
E 14	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	

Schedule H: Cloud Access Service Broker – Background and Requirements

The City of Cape Town currently uses a limited number of cloud services to provide application services to the City of Cape Town staff. In general, tenderers may propose cloud solutions which solve business problems, which comply to City of Cape Town architectural standards.

In addition, in line with best practice the City of Cape Town plans to adopt a multi-cloud strategy for the provision of Infrastructure as a Service (IAAS) and Software as a Service (SAAS). As part of the current scenario planning, the City has selected a limited number of additional cloud services. This is not an indication of commitment, but rather of exploration of future possibilities. These indications are subject to normal tender processes, which are yet to take place.

The City seeks to proactively secure current and future Cloud against common and cloud based risks. Therefore, the City seeks a Cloud Access Service Broker

(CASB) solution to secure City information hosted in Cloud environments, including IAAS, SAAS and PAAS, which integrates in the current environments. The City's uses pfSense servers for authentication and content filtering, and Trend Micro Deep Discovery Web Inspectors (DDWI) for cyber security controls including malware.

This includes access by City owned and managed devices, as well as unmanaged devices from service providers, partners and private devices owned by staff.

Functional 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.

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
H 1	Describe how cloud application discovery project would be conducted to perform an as-is analysis of cloud application usage in order to determine the services currently being used	Netskope can provide visibility into enterprise usage of SaaS and IaaS through our Risk Insights service. This discovery process can occur in several ways, depending on the business use case(s) and deployment method(s) used. (1) For example, cloud app discovery can involve log based discovery on one-time or on-going automated basis, based on firewall, proxy and/or SIEM logs. (2) Additionally, cloud application discovery can be ongoing an ongoing, real-time process when traffic is steered and inspected inline (e.g. "data in motion") using a Forward and/or Reverse Proxy. When inline, user and app/data traffic can be inspected (or "discovered") and acted upon (alerted, blocked, quarantined, encrypted, etc.) on an on-going basis using policies to set rules and triggers. (3) Furthermore, eDiscovery can also be performed for IT-managed or sanctioned applications (most commonly, Office 365, Google App Suite, AWS, Salesforce, Box, etc.) using APIconnectivity (Netskope's API Protection) to gain visibility of content stored in applications (data at rest) and enforce similar policies for visibility and control. Netskope provides a registry of cloud services which includes a risk assessment of each service, named the Netskope Cloud Confidence Index (CCI). The CCI assesses an app's "enterprise readiness" based on objective criteria and then assigns it an overall score. Netskope's CCI tracks over 30,000 cloud services, each measured across 50+ criteria such as: product capabilities, legal, auditing and certifications, and SLAs. Netskope's CCI also includes additional parameters like data privacy, financial stability, and

		other attributes to provide a 360-degree view of a cloud service provider. Based on these factors, an algorithm is applied to determine an overall enterprise- readiness index score- each app is given a score between 0-100. The score gives you an at-a-glance assessment of whether an app is ready for your enterprise, or if you'll need to limit access and permissions to the app based on its risk level. Moreover, you can incorporate the CClinto your cloud app policies within the Netskope Security Cloud Platform - such as to restrict certain activities within the app or limit device types that are allowed to access the app - in order to declare an app suitable for your organization.
H 2	Describe how the CASB offering will integrate with the City's current secure web gateways and proxy servers i.e., pfSense proxy servers and Trend Micro Deep Discovery Web Inspector (DDWI) servers	In Risk Insights mode: Netskope supports closed loop remediation with existing corporate perimeter controls via the capability to create scripts for network equipment, like Blue Coat proxies, Palo Alto Firewalls, Websense Proxies, etc.
		When a customer is in Risks Insights mode (analytics only, no inline deployment), they have the ability to select apps, app categories, apps based on cloud confidence levels (risk criteria) and instruct the Netskope platform to generate a script for the customer's existing perimeter security solution. Risks Insights processing can occur in several ways, depending on the business use case(s) and deployment method(s) used. For example, it may involve log Risks Insights on one-time or ongoing

	automated basis, based on firewall, proxy and/or SIEM logs. Note: It is very rare for a customer to automatically implement policy controls. Netskope does not believe that making unattended changes to enforcement policies is a viable proposition. Changes to policies, especially policies for security solutions, should be reviewed and implemented by a customer's security personnel. When moving to real-time protection modes, the Netskope Security Cloud can become a child (chaining) or split proxy solution (whatever is preferred). Chaining example: the existing proxy chains (i.e. Blue Coat proxy-forwards) to the Netskope Security Cloud for full active real-time control and data security. Netskope is able to provide the Blue Coat administrator with an importable list of managed CASB applications for forwarding to the child proxy. Netskope proposes a trusted model for workflow from Risks Insights to active controls. Split example: the existing proxy's PAC file, when implemented in explicit mode, is downloaded and updated with exceptions after which it's rehosted. The result is a split between web (existing proxy) and cloud app (Netskope Security Cloud) traffic. This integration can provide:
--	---

	• Advance, Enterprise DLP. Organizations need accurate, efficient cloud DLP that leverages their existing investment, and Netskope is considered the most advanced in this regard. The most challenging aspect of DLP management is being able to identify the correct signal from all the noise of false positives. Netskope cancels the noise by employing advanced capabilities such as 3,000+ data identifiers, 25+ predefined legal and regulatory compliance templates, support for 1,000 file types, custom regex, proximity analysis, international support, and fingerprinting, and through the use of context to narrow detection surface area. They make DLP more efficient with critical workflows like quarantine and legal hold, and feature the most elegant integration with on-premises DLP solutions, performing a first pass in the cloud and then tunnelling suspected violations to customers' on-premises solution via secure ICAP. • Surgical visibility and CONTROL for sanctioned AND unsanctioned apps. Rather than take an "allow" or "block" stance to cloud apps, organizations need to say "yes" to useful apps, but just govern the access, activities, and data in sanctioned AND unsanctioned apps. Netskope provides surgical, or fine-grained, visibility and CONTROL for both sanctioned AND unsanctioned apps. For SANCTIONED apps,
--	---

	Netskope provides full-spectrum governance across access, activities, and data, including access based on device class, "least privilege" admin access, and activity-level data governance. For UNSANCTIONED apps, Netskope provides visibility and control at the app, category, or globally with set-it-once policies like "No sharing outside of the company" or "No download of PII to a mobile device." Netskope provides these capabilities across all apps, including native clients on laptops, tablets, and smartphones, and whether users are on-premises or remote.
--	---

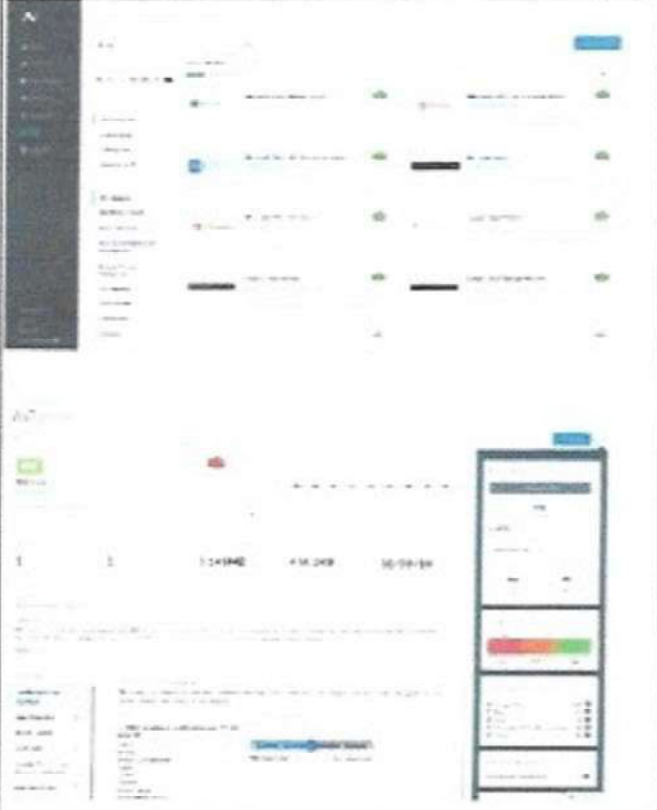
H 3	Which types of Cloud services is your proposed CASB solution able to fully manage. You should consider IAAS, SAAS, and PAAS. Describe each type how they are supported	When deployed inline, in forward-proxy mode, Netskope's CloudXD provides supports for thousands of applications, as well as the ability to map custom applications for detection and policy enforcement. Netskope can control in real time more than 2,400 cloud applications, and that is one of the capabilities that differentiates Netskope from other CASB providers. When deployed inline, in reverse-proxy mode, Netskope's CloudXD supports more than 60 sanctioned applications. Beyond supporting the discovery and protection of data enroute to or from thousands of cloud apps, we also enable a-discovery of sensitive content leveraging vendor APIs to get visibility into usage and data already resident in the service, irrespective of when it was uploaded or where it was created. Netskope's API Protection feature inventories and classifies content, content owners, and collaborators as well as provides content sharing status. You will be able to see if content is private, being shared internally, or being shared publicly. Additionally, it enables you to download files for review, and perform a variety of actions such as restrict access, revoke sharing, encrypt content, quarantine content, and place content on legal hold. Policies can be set up for specific users, groups of users, or all users. Further, you can select file exposure types to look for action to take, and notifications to send out when a policy triggers. Netskope currently has API support for
-----	---	--

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		the following applications:
		IaaS:
		• AWS (CloudTrail & S3) • Microsoft Azure • Google Cloud Platform
		SaaS:
		• Box • Cisco WebEx Teams • Dropbox • Egnyte • Workplace by Facebook • GitHub • Google Gmail • Google Drive • Google Team Drive • Jive • Microsoft Office 365 OneDrive for Business • Microsoft Office 365 Outlook.com • Microsoft Office 365 SharePoint Sites • Microsoft Office 365 SharePoint • Salesforce • Service Now • Slack for Teams • Slack for Enterprise
		Custom Applications
		When deployed in-line, in forward-proxy,

		Netskope also allows to add custom applications via two different mechanisms: • Netskope's Universal connector provides zero-day coverage for new/custom apps in SaaS/IaaS hosted in the public cloud infrastructure (Ex. AWS, GCP, Azure, Rackspace, Softlayer, etc.). The universal connector detects data moving activities like upload/download and crea an application connection so that data protection policies can be enforc • Netskope's Custom connector allows customers to capture the activitie a custom cloud application hosted in a public cloud infrastructure. The output of the captured activities is a JSON file that is ingested by the Netskope platform and allows the administrator to map the specific activities into a custom connector.
H 4	Describe in full how to perform data discovery of sensitive data within a Cloud environment, whether at rest or in movement	Yes. Netskope Risk Insights, Real-time and API Protection modes detect and report on both sanctioned and unsanctioned (Shadow IT) cloud usage in full context, whether Netskope is configured solely for log-discovery, in-line, or both. Risk Insights (Discovery): Netskope identifies over 30,000 cloud apps in its Cloud Confidence Index database. These applications are analysed across 50+ metrics to determine their "enterprise readiness" which classifies the riskiness of these cloud applications. Real-time /Inline Protection:

	Netskope identifies the context and content in any SaaS, IaaS and Web transactions in full context. The platform exposes who, on which machine (managed/unmanaged), where (geo and network location), which app (category, app and app instance) are they using to perform an activity {upload/download/share/login/logout/edit/....} in context (share with whom?) using which content (Data Security, Sensitivity and potential threats). Netskope audits all these events by default, and is able to act upon them using it's inline policy controls. API Protection: Netskope integrates with sanctioned applications using API Protection. This integration exposes and allows control over the context of data at-rest, and allows subscribing to audit logs generated by the respective apps. All event data is available in a consolidated event stream allowing for easy filtering I investigative efforts. All data is also exposed via the Netskope APIs to allow exporting I correlating with 3rd party data and platforms. All events are also fed into Netskope Anomaly engine to identify malicious and anomalous
--	---

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		behaviour in an automated way.
H 5	Describe in full the analytics capabilities to report on all deviations from defined baseline, malware infections, alerts, cloud misconfigurations for IAAS, SAAS and PAAS applications	Yes. Netskope combines cloud visibility and advanced analytics to protect against common threats in the cloud. It leverages a custom rules engine, an advanced anomaly detection platform, and graph analytics to identify threats. Key capabilities include: • Enhanced IaaS visibility based on correlated cloud events such as network traffic, API activity, users, hosts, and more • Advanced, intuitive visualization to accelerate incident investigations and enable proactive hunting • Flexible API capabilities to simplify and automate response

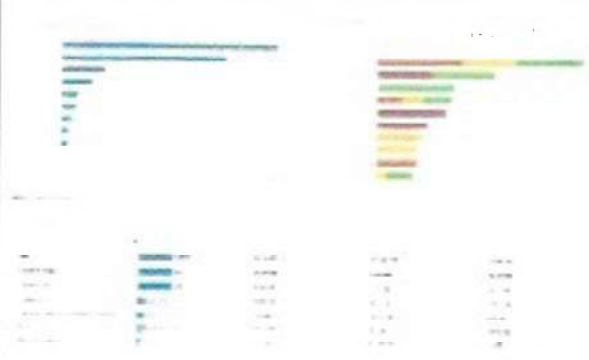
		Continuous Security Assessment for Google Cloud Platform, complementing Netskope's current capabilities for other public cloud environments 
H 6	Describe how visibility and assessment of cloud access, behaviours and sensitive-data handling by end users is provided by the proposed CASB	

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
H 7	Describe how the CASB solution provides usage by category e.g. HCM, Payroll	Yes. The Netskope Security Cloud Platform currently identifies and tracks over 30,000 cloud services across 33 categories, including: • App Admin Console • Application Suite • Business Intelligence and Data Analytics • Business Process Management • Cloud Backup • Cloud Storage • Collaboration • Consumer • Content Management • Customer Relationship Management • Development Tools • E-Commerce Tools • Education • Enterprise Resource Planning • Finance/Accounting • Forums • General • Help Desk Management • HR • IaaS/PaaS • Identity and Access Management • IT Service/Application Management • Knowledge Management • Logistics • Marketing

	• Security • Social • Survey Solutions • Telecom and Call Centre • Web Analytics • Web Design • Web Proxies/Anonymizers • Webmail Information on cloud service usage is presented in numerous ways for different roles within the organization i.e. risk summary, forensic summary, generalized C level summary etc. Additionally, Netskope provides "Advanced Risk Insights" capabilities for thousands of apps where we are able to provide information on activities such as Create, Delete, Download, Edit, Login Attempt, Login Failed, Login Successful, Logout, Post, Share, Upload, View and View All. Activities are normalized across a session and reported on. The Netskope Security Cloud Platform provides you a powerful, user-friendly reporting engine that presents detailed information on your compliance, usage, risk level etc. Netskope's reporting capabilities give you the ability to view pre-defined reports or easily create and save your own custom reports. Predefined Reports Netskope provides over 100 predefined templates that give you the ability to run reports and are displayed in the following dashboards:
--	--

	• Web Usage Summary. This dashboard provides high-level information on the top users with the most usage, top visited categories, top devices used, top browsers used, top blocked users, top blocked sites, and the most visited websites broken down by category (including details on the number of sessions, bytes downloaded, bytes uploaded, and total bytes). • App Usage Summary. This dashboard summarizes the app usage for your company, providing details on how many users are accessing each app, what the Netskope Cloud Confidence Index category is for each app (i.e., excellent, high, medium, low, poor), the number of sessions, bytes downloaded, bytes uploaded, and total bytes. • Risk Exposure Summary. This dashboard provides you insights in the potential risks that your company and users may be exposed to while using cloud-resourced apps. This report provides details on the most used categories and apps by data movement, highest uploads to apps rated medium or below on Netskope's Cloud Confidence Index, and the top apps with risky attributes (such as no SOC 1 or SOC 2 certification, limited to no encryption, no secure password policies, etc.). • Log Usage Summary. This dashboard presents a summary of activity usage patterns, including the most used categories and apps.
--	---

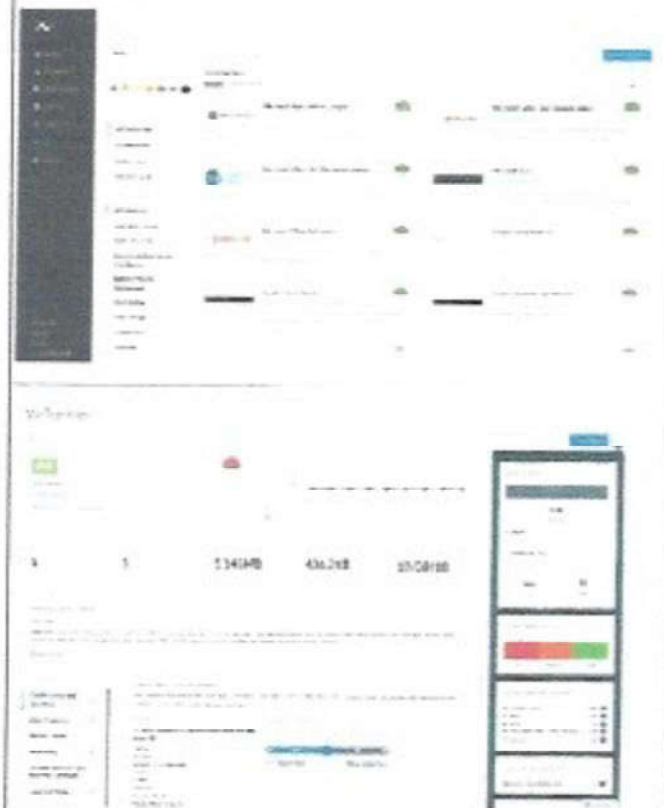
#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		the top users by session and data movement, the top uploaders and downloaders, and sessions and data movement broken down by Cloud Confidence Index category (i.e., excellent, high, medium, low, poor). • Compliance Report. This dashboard provides you insights in the potential risks that your company and users may be exposed to while using cloud applications. Reports include the top non-compliant apps and the users of these apps in use in terms of PCI and HIPAA. It also includes the top apps with risky attributes, such as not supporting encryption at rest, limited data ownership and copyright rights, no SOC certifications. • Cloud Risk Assessment Summary. This dashboard provides information regarding the top users, applications, and categories ranked by session, applications, bytes uploaded, or bytes downloaded. • Cloud Risk Assessment • App Category. This dashboard provides information regarding the top users, applications, and categories ranked by session, applications, bytes uploaded, or bytes downloaded. It also provides numerous metrics regarding the top apps and users broken down into common app categories, including: Cloud Storage, Collaboration, CRM, Finance, HR, and Webmail. • Cloud Risk Assessment -Enterprise

		Readiness. This dashboard provides the top apps ranked by users, bytes downloaded, bytes uploaded, and sessions. • Compromised Credentials. This dashboard provides the top apps and app categories being utilized by users with compromised credentials, as well as those with limited compliance as it relates to HIPAA and PCI. It also displays the top activities being performed by users with compromised credentials. • User Agent Summary. This dashboard provides the top 100 applications ranked by total events.
		

H 8	Describe how the CASB determines a trustability index or assessment. Include the standards assessed against	Netskope provides a registry of cloud services which includes a risk assessment of each service, named the Netskope Cloud Confidence Index (CCI). The CCI assesses an app's "enterprise readiness" based on objective criteria and then assigns it an overall score. Netskope's CCI tracks over 30,000 cloud services, each measured across 50+ criteria such as: product capabilities, legal, auditing and certifications, and SLAs. Netskope's CCI also includes additional parameters like data privacy, financial stability, and other attributes to provide a 360-degree view of a cloud service provider. Based on these factors, an algorithm is applied to determine an overall enterprise- readiness index score-each app is given a score between 0-100. The score gives you an at-a-glance assessment of whether an app is ready for your enterprise, or if you'll need to limit access and permissions to the app based on its risk level. Moreover, you can incorporate the CCI into your cloud app policies within the Netskope Security Cloud Platform - such as to restrict certain activities within the app or limit device types that are allowed to access the app- in order to declare an app suitable for your organization. City of Cape Town can also modify the weightings of these metrics based on your specific business requirements to ensure relevant benchmarking, as well as compare multiple cloud apps side-by-side for further evaluation. Further,
-------------------	--	--

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		City of Cape Town can associate "tags" to identify apps as sanctioned, unsanctioned, used by specific departments, etc. and then apply policies and/or reporting based on these tags. Netskope also assesses the GDPR- readiness of the cloud services and provides a GDPR readiness widget to help you easily identify and report on apps that are not GDPR compliant. The CCI is updated monthly with app update frequency, depending on the popularity of these apps among our customers. Netskope customers can also send feedback regarding the apps directly to us via the service portal (CCI crowd sourcing). A historical overview of each app's CCI trend and the reason why the score has changed in the past is also available.

Please see the examples of the CCI database



and adjustable risk weight values shown below:

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
H 9	Describe how unknown and risky storage of sensitive data is handled by the CASB solution	Netskope does not store any customer end user data (files or structured data), only metadata collected about end user cloud usage. Customer files and structured data are processed by Netskope in memory only and not persisted to disk within our platform environment. The metadata generated and stored by Netskope can include fields such as user name, email address, cloud application instance, Netskope DLP Profile or rule triggered, file name, source and destination IP address, activity/action performed, etc., which is used for our product's events, alerts, and reporting. In general, Netskope does not encrypt this metadata within our data stores, as the data fields captured are not typically considered as "sensitive" and also must be searchable and reportable to support the full functionality and effectiveness of our services and features.
H 10	Describe how the CASB solution will integrate and leverage the City's on-premise Active Directory	Netskope offers our Directory Importer that allows integration with organizations AD or LDAP services to leverage user, group or other attributes. Netskope policy engine can leverage AD user ID's, groups or organization units (OU) to incorporate into a policy decision. This allows administrators to narrow down the users that are fetched from the directory service based on generic AD or LDAP filter constructs. Netskope also supports SCIM, the System for Cross-domain Identity Management which allows users

		to be provisioned to Netskope. You can configure your Azure AD to talk to Netskope using SCIM and push user information that can be used to build policies and reports.
H 11	Describe how access control may be adapted due to the location, time of day, device type: managed or unmanaged	Netskope has device classification capabilities which looks when the access to a cloud application is from a corporate device running the Netskope Client the endpoint can be evaluated using a number of criteria. A corporate (managed) device can be identified by monitoring the Encryption Status, Registry Setting, AV existence(Process), File or Active Directory Domain on the device, OPSWAT. Netskope also supports detecting the presence of an installed client certificate as a way to validate the endpoint is a managed asset. Devices matching/passing these classification checks are considered as managed. Admins can create granular policies which differentiate between managed and unmanaged devices. The Netskope policy engine provides granular policy definition to determine appropriate access that can be based access method, geolocation, OU, Group, user, device, location, end user, app, app instance, category, cloud confidence level, DLP, data classification, activities, device, OS, browser or native client and file object type.

H 12	Describe the challenges how to choose between cloud provider and CASB provided data protection or encryption.	Netskope can integrate with you on premise HSM to enable you to maintain all ownership of your instances key or City of Cape Town can leverage our multi-tenant, cloud based HSM solution to maintain full control of your instance keys. Netskope offers encryption both in-line with traffic (data uploaded) and through API Protection (data at rest in sanctioned applications). Using API introspection, existing content can be encrypted and it will be decrypted transparently for users that have already been provisioned for in-line decryption (and permitted by policy). Encryption of data is a policy based action and can therefore be applied when certain policy criteria are met, including the results of DLP scanning. As an example, an API-based (API Protection) policy could scan data at rest in a cloud application to find PII data in documents and then encrypt only those documents. All transmission of confidential and/or sensitive information over public networks is handled using secured socket layer (SSL). Industry standard strong SSL is used to encrypt data that is sent over the public networks. Supported versions are: TLS version 1.2
------	---	--

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		TLS version 1.3 Netskope Active Cloud DLP works in conjunction with Netskope's API Protection feature, which enables you to discover content resident in your cloud apps, no matter when it was uploaded. Administrators have the option to encrypt the file matching policy violation using Netskope's strong AES-256-bit encryption with support for cloud-based, fault-tolerant FIPS 140-2 Level3 key management with an optional hardware security module or integration with your on-premises, KMIP compliant key management system. Netskope supports multiple structured data encryption methods: • Bring your own Key • Gateway Encryption BYOK (Bring Your Own Key): Netskope acts as key broker between City of Cape Town's or Netskope Cloud hosted HSMs and the SaaS provider. Gateway Encryption: Netskope supports obfuscation and/or encryption of sensitive data for Salesforce.com. With Netskope customers can decide to obfuscate the PII fields creating a one-way hash or apply encryption to protect the content using a customer provided HSM. Since this

		method is no longer actively supported by different SaaS app vendors, Netskope advises to go the BYOK route.
H 13	Describe how the CASB administrative access and activities are recorded for compliance purposes	Admin Actions Netskope provides an Admin Audit Log that can be accessed from the product console. These audit logs can be searched and filtered for admin, activity, timestamp, and severity of the activity. The audit log tracks all activity performed by users/administrators with access to the Netskope product console, including successful and unsuccessful login attempts. The Audit logs record all admin activities such as: • Login • Logout • Policy changes • Setting changes • Add/remove users • Admin privilege changes Additionally, customer admin access logs to our Web Admin UI are logged by our service as event logs and are available to clients within our Web Admin UI. User Activity/Metadata The Netskope Cloud Security platform maintains both real-time analytics of events and alerts generated for unsanctioned and sanctioned apps. The details that are captured in the metadata are: • User ID (both enterprise UserID and any other alias the user used to login to the app)

	• Application • User Location • Application Location • App Instance • Category • Cloud Confidence Level (Enterprise Readiness Score) • DLP Profile and Rule triggered • Data Classification • Policy Name • Activities • Device • OS • Browser or Native Client Used • Device Classification • File Object (like file name or email subject) • Bytes Uploaded • Bytes Downloaded • Length of Connection • Access Method (Reverse Proxy, Forward Proxy, API Protection, Agent, IOS Mobile Profile) • OU • AD Group The exact Activities logged vary between cloud applications. As an example of activities recognized for a few common applications: • Microsoft Office 365 OneDrive for
--	---

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		Business: Create, Delete, Download, Edit, Follow, Login Successful, Post, Share, Upload, View, View All - Box: Create, Delete, Download, Edit, Login Attempt, Login Failed, Login Successful, Logout, Post, Share, Upload, View, View All - Salesforce: Create, Delete, Download, Edit, Follow, Invite, Login Attempt, Login Failed, Login Successful, Logout, Post, Send, Share, Upload, View, View All The Netskope UI presents all events under the SkopelT window which consist of: - Page Events - Application Events - Admin Audit logs • Alerts Incident Management
H 14	List fully supported IAAS Cloud providers supported in South Africa by 31 December 2019. Provide evidence.	Amazon Web Services, Microsoft Azure, and Google Cloud Platform Refer to

H 15	Describe how your proposed CASB solution supports a multimode deployment i.e. forward proxy support, reverse proxy support and API	Yes, Netskope is the only cloud native, multimode CASB as defined by Gartner and fully supports API, in-line proxy (forward and reverse), and log collection. This richness of features and capabilities enables City of Cape Town to meet their cloud security objectives in the most flexible models in the industry. Netskope offers all deployment modes (e.g., log based discovery, API Protection, reverse proxy, every forward proxy method). These options allow Netskope's customers to cover all the ways users access cloud services with granular control - whether on premises or remote, using a laptop or mobile device (managed or unmanaged), and irrespective of access method (browser, sync client or mobile app.) The methods Netskope uses to see cloud service traffic have been patented. Some of the largest companies in the world use Netskope in all modes -including the largest bank, auto maker, insurance company, payments processor, retailer, pharmaceutical,
------	--	---

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		energy company, construction equipment manufacturer, and accountancy firm. Netskope believes that we process more traffic than any other CASB, and we are the only CASB truly governing services using a forward proxy in production at scale. Please see the additional details provided below. Real-time protection • Forward Proxy (GRE, PAC, DNS, Client, Proxy Chaining) for use cases including: - o Real-time visibility and control for managed devices on and off the network accessing sanctioned and unsanctioned cloud services - o Real-time visibility and control for unmanaged devices on the corporate network accessing sanctioned cloud services • Reverse Proxy (SAML, WS-FED, ADFS) for use cases including: - o Real-time visibility and control for unmanaged devices off the corporate network accessing sanctioned cloud services - o Real-time visibility and control for managed devices off the corporate network accessing sanctioned cloud services (not necessary if steering client is installed)

		Out of Band • API Protection for use cases including: - o Data-at-rest (near real time) visibility and control for managed and unmanaged devices accessing sanctioned applications Risk Insights
H 16	Describe how the CASB is able to wrap or proxy, and protect existing custom web applications which have been developed by the City. These web applications are .Net version 4.7	With Netskope's 'custom apps' functionality the admin can define custom services easily and programmatically without any scripting or code development. This provides capability to extend visibility and controls for the security team to understand which users are logging in, logging out, uploading, downloading, or editing in custom apps which can even be hosted in public cloud infrastructure, such as AWS, Azure or GCP. • For the universal connector, once the associated domains for

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		a custom application is added in; administrators can create granular security policies to secure the activities of that custom application. Custom applications also get the same ability as pre-defined applications with respect to being selectively steered for specific platforms. Used in conjunction with Netskope Cloud DLP and Netskope Threat Protection, it is possible to protect sensitive data from leaking from custom cloud services and gain visibility of anomalous end- user behaviours. • For the custom connector, the same features apply, but in this case the administrator must, one-time, capture the actions in the target applications via a browser plugin, and map the output json into specific application actions within the connector.

H17	Describe the DLP capabilities of the solution in order to proactively discover and classify sensitive data. What actions may be taken?	Yes, on SaaS, IaaS and Web with the same advanced engine and the same policy. Netskope has the most advanced DLP in the industry, designed for high accuracy and low false positives, and can be applied to API or inline deployment. Key capabilities include more than 3,000 data identifiers, support for more than 1,000 file types, custom regular expressions, proximity analysis, weighted dictionaries, fingerprinting, exact match, optical character recognition (OCR), and more. You can also respond quickly and thoroughly to DLP policy violations using Netskope's end-to-end workflows and perform forensic analysis with comprehensive, deep activity audit trails. Netskope Cloud DLP supports several workflows that vary based on the nature of the cloud service and the activities available within the service. Admins can block specific actions like upload and share, alert for incident management purposes, quarantine files with sensitive data, encrypt files, and put files in legal hold for review. Furthermore, these actions can be taken based on the severity of the incident. The solution supports four levels of severity - Low, Medium, High, and Critical. The severity level is based on violation counts that are configured on a rule by rule basis.
-----	--	---

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
H18	Describe how sensitive data may be protected when download from a cloud provider to a managed or an unmanaged device. Describe both scenarios.	Policies can be created to prevent opportunity for data exfiltration by creating granular policies that prevent certain types of data (identified by content, file an extension, file type, etc.) from going to unsanctioned cloud applications. Additionally, Netskope's Machine Learning Anomaly Detection (MLAD) is generating actionable insights from the mountain of raw events accumulated. Netskope Active Threat Platform provides advanced machine learning anomaly detection and works behind the scenes using sophisticated machine-learning algorithms to continuously monitor user behaviour. It then intelligently establishes a baseline and uses it to discover anomalous behavioural patterns, which could indicate risky activity. These risky behaviours could be failed logins, unnecessary sharing of credentials, users logging in from risky locations or unknown devices data exfiltration activity such as downloading sensitive data from a sanctioned and then uploading that same content to an unsanctioned app, and many more. The relevant example to this question is our "Data Exfiltration" anomaly, which tracks when a file (MD5) has been subsequently uploaded to a service that is different than that from which it had been previously downloaded within a fixed duration of time (e.g. "John downloaded a file

		form Box, and then uploaded that same file to Gmail within 1 hour").
H19	Describe how the proposed CASB solution will integrate with the existing McAfee ESM SIEM solution	Netskope offers a REST API interface that allows you to leverage events and alerts obtained from the deep visibility provided by the platform. Organizations use this interface to incorporate this data into existing processes that have been defined as part of SIEM technologies. We have been successfully deployed with many leading SIEM providers such as ArcSite, Splunk, and QRadar. Netskope has developed a Splunk App that provides a dashboard to view cloud security events, as well as searching of all of the events generated. The Netskope Security Cloud platform maintains
		both real-time analytics of events and alerts generated. Netskope also provides a simple abstraction script to convert the REST API data to other formats such as syslog for those that require it.

H20	Describe how the proposed CASB solution will integrate with your proposed enterprise DLP solution, or other enterprise DLP solutions.	The Netskope solution can integrate seamlessly with an ICAP interface to City of Cape Town Onpremise DLP solution. This will require to deploy a virtual appliance (secure forwarder) that will mediate the connection between the Netskope platform and the existing on-prem DLP. Netskope has the most advanced DLP in the industry, designed for high accuracy and low false positives, and can be applied to both Inline and API deployments. Key capabilities include more than 3,000 data identifiers, support for more than 1,000 file types, custom regular expressions, proximity analysis, weighted dictionaries, fingerprinting, exact match, optical character recognition (OCR), and more. Netskope has been successful in working with many customers on migrating on-prem DLP policies to its cloud DLP.
H21	Describe how the proposed solution will limit or restrict poor cloud applications and recommend more secure or trustworthy applications to the user directly	Yes. Netskope provides a registry of cloud services which includes a risk assessment of each service, named the Netskope Cloud Confidence Index (CCI). The CCI assesses an app's "enterprise readiness" based on objective criteria and then assigns it an overall score. Netskope's CCI tracks over 30,000 cloud services, each measured across 50+ criteria such as: product capabilities, legal, auditing and certifications, and SLAs. Netskope's CCI also includes additional parameters like data privacy, financial stability, and other attributes to provide a 360-degree view of a cloud service provider. Based on these factors, an algorithm is applied to determine an overall enterprise-readiness index score -each app is given a score between 0-100.

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		The score gives you an at-a-glance assessment of whether an app is ready for your enterprise, or if you'll need to limit access and permissions to the app based on its risk level. Moreover, you can incorporate the CCI into your cloud app policies within the Netskope Security Cloud Platform - such as to restrict certain activities within the app or limit device types that are allowed to access the app - in order to declare an app suitable for your organization. City of Cape Town can also modify the weightings of these metrics based on your specific business requirements to ensure relevant benchmarking, as well as compare multiple cloud apps side-by-side for further evaluation. Further, City of Cape Town can associate "tags" to identify apps as sanctioned, unsanctioned, used by specific departments, etc. and then apply policies and/or reporting based on these tags. Netskope also assesses the GDPR- readiness of the cloud services and provides a GDPR readiness widget to help you easily identify and report on apps that are not GDPR compliant. The CCI is updated monthly with app update frequency, depending on the popularity of these apps among our customers. Netskope customers can also send feedback regarding the apps directly to us via the service portal (CCI crowd

		sourcing). A historical overview of each app's CCI trend and the reason why the score has changed in the past is also available. Please see the examples of the CCI database and adjustable risk weight values shown below:
		 

H22	Describe and provide overall architectural diagrams how the proposed CASB solution will be implemented on premise and in cloud	Depending on your use case and requirements, one or more deployment modes could be deployed. Netskope Risk Insights can be deployed as a SaaS only solution. However, it is typical for a customer to install a Virtual Appliance to collect logs from the web proxy, parse the logs, and then upload the logs to the Netskope cloud. The Netskope Virtual Appliance is an image that can be hosted on VMware ESX, KVM, AWS or Microsoft Hyper-V. Alternatively, and at an additional cost, Netskope is the only CASB to offer physical appliances. They have been built by Netskope and come in a tamper-resistant chassis. These appliances support different modes of deployment, including Risk Insights, Inline Policy Enforcement (Forward Proxy), and Inline Traffic Steering. Netskope supports the following inline options (all can be done simultaneously): 1. Proxy-Chaining- You can configure your on premise perimeter proxy to point to Netskope as an upstream proxy and steer explicit application to your instance of the Netskope platform for real-time contextual access control, policy control, data protection, and governance. 2. Netskope Virtual Appliance - can be configured in various operational modes to include ICAP DLP client, KMIP Client, Explicit Proxy or in DNS integration mode which will allow traffic going to SaaS apps to be steered through this virtual appliance to your instance of Netskope in the cloud.
-----	--	---

3. Netskope Reverse Proxy- Provides support for your managed and unmanaged users access sanctioned SaaS services through browser sessions. There is nothing to deploy on premise for this mode of operation.

4. Netskope Mobile Profile- Allows Netskope to deploy a profile or integrate with your MOM solutions to steer traffic to your instance of Netskope for any SaaS app.

5. SAML integration- This is ideally used to impose granular policies over unmanaged endpoints.

6. Netskope Client - Users with the Netskope client will have their designated SaaS traffic steered through your instance of Netskope.

There is nothing to deploy on premise for this mode of operation. The Netskope client runs at user level context and uses Admin level privileges for the installer service. The "NS Agent Service" will be loaded only on restarting the Netskope client drive, not during enabling/disabling or network flaps. Netskope client does not interfere with or modify anything specific in the Native OS Network stack, it just captures and tunnels the SaaS traffic. The Netskope client runs in minimal CPU and memory and is supported on the following:

- Windows 7, Windows 8, Windows 8.1, Windows 10 (32 and 64 bit)

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
		• MacOS 10.8 (Mountain Lion), Mac 10.9 (Mavericks) and Mac 10.10 (Yosemite), Mac 10.11 (El Captain), MacOS 10.12 (Sierra), Mac 10.13 (High Sierra), Mac 10.14 (Mojave) • iOS 10.0 and above • Android 5.0 (Lollipop), Android 6.0 (Marshmallow), Android 7.0 (Nougat), Android 8.0 (Oreo) • Chrome OS version 53 and above Additionally, the Netskope solution is able to integrate in other ways as well, such as GRE and IPSec Tunnels. Please see the attached document which outlines deployment options.

H23	Describe the your proposed CASB solution support for SAP Success Factors HR cloud suite solution	SAP Success Factors is supported in forward proxy mode. The following activities can be detected Create, Delete, Download, Edit, Login Attempt, Login Failed, Login Successful, Logout, Share, Upload, View And the supported actions are: - Granular access control - DLP - Threat Protection The following remediation actions can be enforced (may vary depending on the activity): -Alert -Allow -Block -User Alert - Quarantine SAP Success Factors Community is also supported with granular access control for the following actions: Download, Login Attempt, Login Failed, Login Successful, Logout, Upload Netskope is working to an API connector for SAP Success Factors
-----	--	--

#	CASB systems - Technical Requirements / Questions	Brief Description / Technical Response
H24	Is the proposed CASB solution cloud component hosted in South Africa in order to minimize latency.	Yes, Netskope has a Point of Presence in Johannesburg (JNB1) and is hosted within Liquid Telecom
H25	How will the proposed solution integrate with the City's Palo Alto firewalls?	Netskope can consume logs from these supported technologies: Cisco-ASA, Bro- IDS, Checkpoint, Cisco Catalyst, Cisco IronPort, Fortinet, Bluecoat, Microsoft-ISA, Juniper SRX, McAfee, Juniper Netscreen, Palo Alto Networks, Blue Coat proxySG, Cisco ScanSafe, Sensage SIEM, Sonicwall, Sophos Web Gateway, Symantec Web Security, Trustwave, Websense, Zscaler. In addition to the above built-in parsers, Netskope also supports creating custom parsers online for custom log formats (CSV, syslog, and SIEM exports).
H26	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	Company policy depicts that Coronation may not provide written references, however you may contact Philip Greeff on Greeff@coronation.com or 021 680 2404 for a reference on CASB (Netskope) and Managed Security Operations Centre (Nview)