OPERATOR AGREEMENT

NEVADA CLOUD | 190 CIRCULAR DRIVE • LORRAINE • PORT ELIZABETH • 6070 • SOUTH AFRICA

NEVADA CLOUD | PROTECTION OF PERSONAL INFORMATION ACT | OPERATOR AGREEMENT

entered into between:

Party A (Responsible Party)

_____

_____

And

Party B (Operator)
Nevada Cloud (PTY) LTD

TABLE OF CONTENTS

1. **RECITAL**

1.1. The Parties hereby agree that in the case of any Contract or ongoing relationship between the Parties, and where the provisions of POPIA apply to the Processing of Personal Information in relation to the Services, these terms and conditions shall apply to and supplement the terms and conditions of such Contract.

1.2. In the event of a conflict between the provisions of this Agreement and the/a Contract, the provisions of this Agreement will take precedence in regard to all aspects pertaining to any Processing of Personal Information by the Operator of any Data Subjects for the Responsible Party.

2. **DEFINITIONS AND INTERPRETATION**

2.1. "**Agreement**" means this Protection of Personal Information Act Operator Agreement;

2.2. "**Affiliate**" means with respect to a Party any person, partnership, joint venture, corporation or other form of enterprise, domestic or foreign, including but not limited to Subsidiaries and associates that directly or indirectly, Control, are Controlled by, or are under common Control with a Party. For purposes of this Agreement, the term "Subsidiaries" shall have the meaning ascribed thereto in the *Companies Act, 2008*;

2.3. "**Business Day**" means any day from Monday to Friday and excludes any public holiday as gazetted in the Republic of South Africa;

2.4. **Confidential Information**" means any information or data of any nature, tangible or intangible, oral or in writing and in any format or medium, which (i) by its nature or content is, or ought reasonably to be identifiable as, confidential and/or proprietary to the Responsible Party or a third party associated to the Responsible Party, or (ii) is provided or disclosed in confidence, and which the Responsible Party or any person acting on behalf of the Responsible Party may disclose to the Operator, or (iii) may come to the knowledge of the Operator by whatsoever means. Without limitation, Confidential Information shall include the following:

2.4.1. information relating to the Responsible Party's business activities, business relationships, products, services, processes, data, and Staff, including agreements to which the Responsible Party is a party (including this Agreement);

2.4.2. information contained in or constituting or relating to the Responsible Party's technology and telecommunications systems including third party hardware and software, and associated material, and information or incidents concerning faults or defects therein;

2.4.3. the Responsible Party's technical, scientific, commercial, financial and market information, methodologies, formulae and trade secret;

2.4.4. the Responsible Party's architectural information, demonstrations, plans, designs, drawings, processes, process maps, functional and technical requirements and specifications and the data relating thereto;

2.4.5. Intellectual property that is proprietary to the Responsible Party or that is proprietary to a third party;

2.4.6. information relating to the Responsible Party's current and existing strategic objectives, strategy documents and plans for both its existing and future information technology, processing, business processing and business process outsourcing; and

2.4.7. Personal Information.

2.5. "**Contract**" means any agreement and any annexures or schedules thereto, entered into between the Parties in respect of the provision of Services by the Operator to the Responsible Party;

2.6. "**Control**" means the ability, by virtue of ownership, right of appointment, voting rights, management agreement, or agreement of any kind, to control or direct, directly or indirectly, the board or executive body or decision-making process or management of such entity;

2.7. "**Data Subject**" means any person to whom the specific Personal Information relates, as contemplated in POPIA;

2.8. "**Information Officer**" means the appointed information officer of the Responsible Party from time to time, being, as at the Signature Date, (insert name);

2.9. "**Operator**" has the meaning set out in POPIA and for purposes of this Agreement means Party B with registration number 2016/159603/07 and any authorised subcontractor of that party;

2.10. "**Party**" or "**Parties**" means either the Responsible Party or the Operator or both, as the context may require;

2.11. "**Personal Information**" has the meaning set out in section 1 of POPIA, and includes special personal information as defined in section 26 of POPIA and relates only to Personal Information obtained by the Operator as a result of the Contract;

2.12. "**POPIA**" means the *Protection of Personal Information Act, 2013*;

2.13. "**Processing**" has the meaning set out in POPIA and includes any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including:

2.13.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.13.2. dissemination by means of transmission, distribution or making available in any other form; or

2.13.3. merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information,

the details of which are set out in Schedule 2;

2.14. "**Responsible Party**" has the meaning ascribed thereto in POPIA, and for purposes of this Agreement shall mean Party A with registration number [insert number]

2.15. "**Security Compromise**" means an incident where there has been, or there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person with reference to the Operator's use of the Personal Information under this Agreement;

2.16. "**Services**" means any supply or rendering of services by the Operator for the Responsible Party in terms of a Contract and in terms of which the Operator *inter alia* Processes Personal Information of Data Subjects;

2.17. "**Signature Date**" means the date of signature of this Agreement by the last Party to do so in time; and

2.18. "**Staff**" means any employee, independent contractor, agent, consultant, subcontractor or other representative of either Party.

3. INTERPRETATION

In this Agreement:

3.1. Words importing:

3.1.1. any one gender includes the other gender;

3.1.2. the singular includes the plural, and vice versa; and

3.1.3. natural persons include created entities (corporate or unincorporated) and vice versa.

3.2. Any reference to "days" shall be construed as being a reference to calendar days unless qualified by the word "business". When any number of days is prescribed in this agreement, same shall be reckoned exclusively of the first and inclusively of the last day unless the last day falls on a Saturday, Sunday or public holiday in the Republic of South Africa, in which case the last day shall be the next succeeding day which is not a Saturday, Sunday or public holiday in the Republic of South Africa.

3.3. The words "include", "includes", and "including" means "include without limitation", "includes without limitation", and "including without limitation". The use of the word "including" followed by a specific example/s shall not be construed as limiting the meaning of the general wording preceding it.

3.4. Any substantive provision, conferring rights or imposing obligations on a Party and appearing in any of the definitions in clause 3 or elsewhere within the Agreement, shall be given effect to as if it were a substantive provision within the body of the Agreement.

3.5. Terms other than those defined in the Agreement and terms appearing in the lower case but which in the title case are defined in the Agreement, will be given their plain English meaning.

3.6. Any Party shall, where relevant, be deemed to be references to, or to include, as appropriate, their respective successors or permitted assigns.

3.7. References to statutory provisions shall be construed as references to those provisions as respectively amended, consolidated, extended or re-enacted from time to time and shall be construed as including references to the corresponding provisions of any earlier legislation directly or indirectly amended, consolidated, extended or replaced by those statutory provisions or re-enacted and shall include any orders, ordinance, regulations, instruments or other subordinate legislation made under the relevant statute.

3.8. Expressions defined in the main body of this Agreement shall bear the same meanings in schedules to this Agreement which do not themselves contain their own conflicting definitions.

3.9. If figures are referred to in numerals and in words in this Agreement and if there is any conflict between the two, the words shall prevail.

4. **COMMENCEMENT AND DURATION**

This Agreement shall commence on the Signature Date hereof and shall continue to be of force and effect for as long as the Operator remains in possession of any Personal Information of the Data Subjects, regardless of any expiration or termination of a Contract.

5. **PROCESSING BY THE OPERATOR**

5.1. It is recorded that, pursuant to its obligations under this Agreement, the Operator will Process Personal Information of Data Subjects (i) in connection with and for the purposes of the provision of the Services and (ii) strictly in accordance with the processing limitations set out in Schedule 1 and will act as the Operator for purposes of POPIA.

5.2. The Operator acknowledges and agrees that the Responsible Party retains all right, title and interest in and to the Personal Information and that the Personal Information shall constitute the Responsible Party's Confidential Information.

5.3. Unless required by law, the Operator shall Process the Personal Information only:

5.3.1. in compliance with this Agreement; and

5.3.2. for the purposes connected with the provision of the Services or as specifically otherwise instructed or authorised by the Responsible Party in writing.

5.4. If the Operator is ever unsure as to the parameters or lawfulness of the instructions issued by the Responsible Party, the Operator will, as soon as reasonably practicable, revert to the Responsible Party for the purpose of seeking clarification or further instructions.

5.5. The Operator shall co-operate and assist the Responsible Party with consultations with or notifications to relevant regulatory authorities and/or Data Subjects that the Responsible Party considers are relevant pursuant to POPIA in relation to the Personal Information.

5.6. The Operator shall treat the Personal Information that comes to its knowledge or into its possession as confidential and shall not disclose it without the prior written consent of the Responsible Party, unless required to do so by law. For avoidance of doubt, the provisions of the Contract in relation to Confidential Information or any non-disclosure agreement, or the provisions regarding confidentiality contained in any Contract, as the case may be, entered into between the Parties shall with the necessary changes, apply to this Agreement.

5.7. Without limiting the Operator's obligations under this Agreement, the Operator shall comply with the Responsible Party’s data privacy and protection policies, applicable industry or professional rules and regulations, in relation to the safeguarding of Personal Information,

which may apply to it and take steps to keep abreast and ensure that it and its Staff comply fully with all applicable laws and regulations that are applicable to the Agreement.

6. **SECURITY**

6.1. The Operator undertakes to Process Personal Information in accordance with the Responsible Party's technical and organisational security measures as set out in Schedule 3 or agreed to by the Parties.

6.2. The Operator shall secure the integrity and confidentiality of Personal Information provided by the Responsible Party by taking appropriate, reasonable technical and organisational measures to prevent:

6.2.1. loss of, damage to or unauthorised destruction of personal information;

6.2.2. unlawful access to or processing of personal information; and

6.2.3. must take reasonable measures to:

6.2.3.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

6.2.3.2. establish and maintain appropriate safeguards against the risks identified;

6.2.3.3. regularly verify that the safeguards are effectively implemented; and

6.2.3.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

6.3. Within 5 (five) Business Days of a request from the Responsible Party, the Operator shall provide to the Responsible Party a written explanation and full details of the technical and organisational measures taken by or on behalf of the Operator to demonstrate and ensure compliance with this clause 6.

7. **SECURITY COMPROMISE**

7.1. The Operator shall notify the Responsible Party in writing immediately and in any event, no later than 24 (twenty-four) hours if there has been a Security Compromise.

7.2. The Operator shall as soon as is reasonably possible investigate the Security Compromise and furnish the Responsible Party with:

7.2.1. a preliminary report within 24 (twenty four) hours from its initial notification to the Responsible Party in terms of clause 7.1 above setting out the details of the Data Subjects affected by the Security Compromise and the nature and extent of the Security Compromise, including details of the identity of the unauthorised person who may have accessed or acquired the Personal Information; and

7.2.2. daily reports on progress made at resolving the compromise.

7.3. The Operator shall take reasonable steps to mitigate the effects and to minimise any damage resulting from the a Security Compromise and assist the Responsible Party in remediating or mitigating any potential damage from the breach to the extent that such remediation or mitigation is within the Operator's control as well as reasonable steps to prevent a recurrence of such a Security Compromise, including interviewing and the possible removal of staff from the performance of Services for the Responsible Party.

8. OPERATOR STAFF

The Operator shall:

8.1. limit the Processing of and access to the Personal Information to those Staff who need to know the Personal Information to enable the Operator to render the Services;

8.2. ensure that its Staff will not Process Personal Information: (i) except in accordance with the provisions of this Agreement; and (ii) procure that its Staff are contractually obligated to maintain the security and confidentiality of any Personal Information and this obligation continues even after their engagement ends; and

8.3. take all reasonable steps to ensure the Staff Processing Personal Information receive adequate training on compliance with this Agreement and POPIA applicable to the Processing.

9. ACCESS REQUESTS

9.1. The Operator shall provide the Responsible Party with full co-operation and assistance in relation to any requests for access to, correction of or complaints made by the Data Subjects relating to their Personal Information.

9.2. The Operator shall notify the Responsible Party in writing:

9.2.1. within 3 (three) Business Days of receipt thereof, of any request for access to or correction of the Personal Information or complaints received by the Operator relating to the Responsible Party's obligations in terms of POPIA and provide the Responsible Party with full details of such request or complaint; and

9.2.2. promptly of any legally binding request for disclosure of Personal Information or any other notice or communication that relates to the Processing of the Personal Information from any supervisory or governmental body.

10. AUDIT RIGHTS

10.1. The Responsible Party or its agent shall have the right to audit the Operator at any time, with reasonable notice, if there is a reasonable suspicion that the Operator is not complying with the provisions of this Agreement or where there is a suspicion that the confidentiality, integrity and accessibility of Personal Information is likely to be compromised. Such audit rights shall include the right of access to systems, procedures and software, and inspection of the physical security of the Operator's premises.

10.2. The Operator shall offer reasonable assistance and co-operation to the Responsible Party and/or its auditors or inspectors in the carrying out of such auditing exercise.

10.3. To the extent that the Operator engages an independent auditor in relation to the provisions of applicable data privacy and protection legislation to carry out an audit of its operations, the Operator agrees to provide the Responsible Party with copies of the audit reports of all such audit exercises.

10.4. Nothing in this clause 10 should be read as providing the Responsible Party with unlimited access to audit the Operator without just cause.

11. SEPARATION OF PERSONAL INFORMATION

The Operator shall Process the Personal Information in relation to the Services separately from Personal Information, data and property relating to the Operator or any third party, and may not be combined or merged with information of another party unless otherwise agreed to in writing by the Responsible Party.

12. RETURN AND RETENTION OF PERSONAL INFORMATION

12.1. The Responsible Party may, at any time on written request to the Operator, require that the Operator immediately return to it any Personal Information and may, in addition, require that the Operator furnish a written statement to the effect that upon such return, it has not retained in its possession or under its control, whether directly or indirectly, any such Personal Information or material.

12.2. Alternatively, the Operator shall, as and when required by the Responsible Party on written request, destroy all such Personal Information and material and furnish the Responsible Party with a certificate of destruction to the effect that the same has been destroyed, unless the law

prohibits the Operator from doing so. In that case, the Operator agrees that it will maintain the confidentiality of the Personal Information and will not actively Process the Personal Information any further.

12.3. The Operator shall comply with any request in terms of this clause 12 within 7 (seven) days of receipt of such request.

13. **SUBCONTRACTING**

13.1. The Operator may not subcontract the performance of any of its obligations under this Agreement without the Responsible Party's prior written consent having been obtained. All references to the Operator's Staff shall be deemed to include the employees of any subcontractor of the Operator.

13.2. In the event that the Responsible Party agrees to the Operator subcontracting certain or all of the Operator's obligations, the Operator must only do so by way of a written contract with the subcontractor which contract must impose the same obligations on the subcontractor as are imposed on the Operator in terms of this Agreement insofar as the Processing of Personal Information by the subcontractor is concerned.

14. **CROSS-BORDER DATA TRANSFER**

14.1. It is hereby recorded and agreed that in order for the Operator to be able to fulfil its obligations in terms of the Contract, it may be necessary for the Operator to transfer Personal Information to a third party outside of South Africa.

14.2. In the event of such cross-border transfer, the Operator hereby warrants and undertakes in favour of the Responsible Party that:

14.2.1. it shall procure the third party's compliance with all the obligations of this Agreement insofar as the Processing of Personal Information by the third party is concerned;

14.2.2. the Operator shall at all times be responsible to the Responsible Party for fulfilment of all the Operator's obligations under the Contract and remain the Responsible Party's sole point of contact regarding the Services, including with respect to payment;

14.2.3. the third party is prevented from further transferring Personal Information to other third parties;

14.2.4. it shall ensure that the third party has implemented the appropriate technical and organisational security measures in the relevant jurisdiction in which the Personal Information is being transferred, as contained in Schedule 3; and

14.2.5. it has implemented and taken technical and organisational security measures to safeguard the security of the Personal information in-transit.

14.3. The Operator hereby agrees that the Responsible Party shall solely hold it responsible for the fulfilment of all obligations under this Agreement and it hereby indemnifies and holds the Responsible Party harmless from any and all losses arising from any claim or action brought against the Responsible Party by any party, including by any regulator, arising from or due to the Operator's or the offshore third party's breach of the obligations contained in this Agreement in relation to the lawful Processing of Personal Information in South Africa or anywhere else in the world.

15. CONFIDENTIALITY

15.1. The Operator agrees and undertakes:

15.1.1. except as permitted by this Agreement, not to disclose or publish any Confidential Information in any manner for any reason or purpose whatsoever without the prior written consent of the Responsible Party and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Operator to obtain the consent of such third party;

15.1.2. except as permitted by this Agreement, not to utilise, employ, exploit or in any other manner whatsoever use the Confidential Information for any purpose whatsoever without the prior written consent of the Responsible Party and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Operator to obtain the consent of such third party;

15.1.3. to restrict the dissemination of the Confidential Information to only those of its Staff who are actively involved in activities for which use of Confidential Information is authorised and then only on a “need to know” basis and the Operator shall initiate, maintain and monitor internal security procedures reasonably acceptable to the Responsible Party to prevent unauthorised disclosure by its Staff; and

15.1.4. to take all practical steps, both before and after disclosure, to impress upon its Staff who are given access to Confidential Information the secret and confidential nature thereof.

15.2. The obligations of the Operator with respect to each item of Confidential Information shall endure for an indefinite period from receipt of that item of Confidential Information. The obligations referred to in this clause 15 shall endure notwithstanding any termination of this Agreement, any other agreement entered into between the Parties or any discussions between the Parties.

15.3. The Operator hereby indemnifies and holds the Responsible harmless from any and all losses arising from, or in connection with, any claim or action arising from the Operator's breach of any obligation with respect to Confidential Information.

16. RESPONSIBLE PARTY AFFILIATES

Unless otherwise agreed to the contrary, the Parties hereby agree that any Affiliate of the Responsible Party shall be entitled to rely on all the provisions of this Agreement, which provisions are binding between the Affiliate of the Responsible Party and the Operator, in respect of any contract that might be entered into between the Operator and the Affiliate of the Responsible Party in terms of which the Operator will be Processing Personal Information on behalf of the Affiliate of the Responsible Party. For the avoidance of doubt, this Agreement is applicable and binding in respect of all contracts concluded between the Operator and the Responsible Party or the Affiliate of the Responsible Party where the Operator Processes Personal Information on behalf of the Responsible Party or the Affiliate of the Responsible Party.

17. INDEMNITY

17.1. The Operator hereby indemnifies the Responsible Party in respect of all losses, claims, damages, costs, expenses, fines and penalties arising from and in connection with the Operator's (including its Staff) actions and/or omissions relating to this Agreement.

17.2. Any financial caps or limitation of liability set out in the Contract shall not apply to this indemnity.

18. BREACH AND TERMINATION

18.1. In the event of either of the Parties committing a breach of any of the conditions of this Agreement and failing to remedy such breach within 7 (seven) Business Days of receipt of a notice from the other Party requesting it to remedy such breach, then the other Party shall be entitled to cancel this entire Agreement forthwith and claim such losses as it may have

suffered. In the event of termination of this Agreement, the Party terminating this Agreement shall have a right to also exercise its rights of termination under the Contract.

18.2. Notwithstanding anything to the contrary contained in this Agreement, the Parties shall be entitled to terminate this Agreement by mutual agreement in writing.

18.3. The provisions of this clause 18 shall not affect or prejudice any other rights/remedies which the Parties may have in law or in any other Contract between the Parties.

19. **CONSEQUENCES OF TERMINATION**

19.1. The termination of this Agreement shall not affect the rights of either of the Parties that accrued before termination of this Agreement or which specifically survives the termination of the Agreement.

19.2. Upon termination of this Agreement or upon request by the Responsible Party, the Operator shall return or destroy any material containing, pertaining or relating to the Personal Information disclosed pursuant to this Agreement to the Responsible Party in terms of clause 12 unless the law prohibits the Operator from doing so. In that case, the Operator agrees that it will maintain the confidentiality of the Personal Information and will not, under any circumstance, Process the Personal Information any further.

20. **WAIVER**

20.1. Failure or delay by either Party in exercising any right will not constitute a waiver of that right.

20.2. No waiver of any of right under this Agreement will be binding unless it is in writing and signed by the Party waiving the right.

21. **SEVERABILITY**

If any part of this Agreement is found to be invalid or unenforceable, it shall be severed from the remainder of this Agreement, which shall remain valid and enforceable.

22. **CESSION AND DELEGATION**

The Operator may not cede its rights or delegate its obligations in terms of this Agreement, without the prior written consent of the Responsible Party, which consent shall not be unreasonably withheld.

23. GOVERNING LAW AND JURISDICTION

23.1. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed exclusively in accordance with South African law.

23.2. The Operator consents and submits to the jurisdiction of the High Court of South Africa, Gauteng Local Division, Johannesburg in any dispute arising from or in connection with this Agreement. Without prejudice to any other rights or remedies which the Responsible Party may have, the Operator acknowledges that nothing herein shall preclude the Responsible Party from seeking urgent relief or specific performance from a court of competent jurisdiction.

24. NOTICES AND DOMICILIUM

24.1. The Parties choose the following addresses as their respective *domicilia citandi et executandi* for purposes of giving any legal notice and serving any legal process:

24.2. **Responsible Party:**

Physical address: _____

Email: _____

Attention: Information Officer

24.3. **Operator:**

Physical address: 190 Circular Drive, Lorraine, Port Elizabeth, 6070, South Africa

Email: info@nevadacloud.com

Attention: Russell Meyer-Wilson

Any notice addressed to a Party at its physical or postal address shall be sent by prepaid registered post or delivered by hand.

24.4. Any notice shall be deemed to have been given and received:

24.4.1. if posted by prepaid registered post, 7 (seven) days after the date of posting thereof.

24.4.2. if hand delivered, on the day of delivery; and

24.4.3. if sent by email on the first Business Day after the date of transmission.

24.5. Notwithstanding anything to the contrary contained in this clause 24 a written notice or communication actually received by a Party shall constitute adequate written notice or communication to it notwithstanding that it was not sent or delivered to its chosen domicilium citandi et executandi or in the manner provided in this clause 24.

25. WHOLE AGREEMENT

This Agreement constitutes the whole of the agreement between the Parties hereto relating to the subject matter hereof and the Parties shall not be bound by any terms, conditions or representations whether written, oral or by conduct and whether express or tacit not recorded herein.

26. COUNTERPARTS

This Agreement may be executed in counterparts, each of which will be an original and which together constitute the same agreement.

PARTY A

Signature: _____

who warrants that he / she is duly authorised thereto

Name: _____

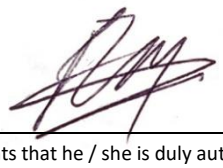
Date: _____

Place: _____

Witness: _____

Witness: _____

PARTY B

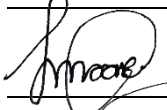
Signature:  _____

who warrants that he / she is duly authorised thereto

Name: Russell Meyer-Wilson

Date: 29-6-2021

Place: Port Elizabeth

Witness:  _____

Witness:  _____

Schedule 1 PROCESSING LIMITATIONS

The Operator may Process Personal Information as follows:

Processing activity	Allowed (Yes/No)	Extent of processing / additional requirements
Collecting	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Receiving	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Recording	No	
Organising	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Collation	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Storage	Yes	All storage is subject to the security safeguards as set forth in Schedule 3.
Updating	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Modification	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A

Retrieval	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Alteration	No	
Consultation	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Use	No	Solely as contemplated in this Schedule 1 and for the provision of the Services.
Dissemination by means of transmission	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Distribution	No	
Making available in any other form	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Merging	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Linking	Yes	In rendering the Services in accordance with the provisions of the service agreement and/or addendums or SOW's with Party A
Restriction	No	
Degradation	No	
Erasure	Yes	If authorised pursuant to clause 12.
Destruction	Yes	If authorised pursuant to clause 12.

Schedule 2 DETAILS OF THE PROCESSING

Data Subjects

The Personal Information Processed concern the following Data Subjects:

1. Employee Information (Includes Employees, Ex-employees, contingent workers (active and terminated, Agents (active and terminated)
2. Parties to Business (Suppliers, Customers, Entities, affiliates etc.) of the responsible party.

Purpose of Processing

1. The primary purpose of processing rights given to the operator is to enable the operator to deliver contractual obligations and meet agreed service level agreements without compromising on responsible party's compliance needs.
2. In rendering the Services in accordance with the provisions of the service agreement with the responsible party, the operator complies with all applicable Laws and regulation for the duration of this agreement.

Categories of data

The Personal Information transferred concern the following categories of data:

1. Employee, and/or Subscriber, and/or partner Data Categories:
2. Classified business information

Details of the Data Subject's Special Personal Information:

_____

_____

_____

_____

_____

Schedule 3 TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

People, awareness, and training

- Employees with access to the Personal Information to sign a NDA.
- Regular awareness training on POPIA for all employees with access to the Personal Information.
- The Operator must, on request by the Responsible Party, demonstrate its technology security education, training and awareness programmes that shall ensure that all users are aware of security threats and concerns; and are equipped to apply organisational security policies and principles at all times.
- Personal accountability for technology security shall be incorporated in the organisational structures to ensure that every individual applies the applicable security policies, principles, procedures, and practices in his/her daily work-related activities in protecting the organizations information resources.
- Any parties accessing the Responsible Party's information resources are required to acknowledge acceptance of and intention to comply with its acceptable use & access control procedure as stipulated in its Technology Security Policy.
- The Operator's information assets shall be classified according to their criticality to classification requirements defined within the Operator's information classification policy so as to enable an appropriate level of protection.
- If parties\users that need access to information which requires additional protection, in accordance with the classification, such access shall only be granted once such protection has been provided.
- Access shall only be provided for the period during which it is required, and all access shall be formally authorised.

Organisation control

- Internal data privacy policies and procedures which comply with requirements of POPIA.
- The data privacy policy covers all Personal Information Processed by the Operator to access information resources.
- Data privacy is implemented and audited for compliance on an annual basis.
- All parties\users must only lawfully and in a reasonable manner Process Personal Information that is adequate, relevant, and not excessive for the business purposes for which it is to be used.
- All parties\users must take reasonable steps, including physical, administrative, and technical safeguards, to protect Personal Information from loss, misuse, unauthorised access, disclosure, alteration or destruction.

- All parties\users must take reasonable steps to ensure that Personal Information is retained only for as long as needed to meet the purposes for which it was collected and in accordance with the Operator's data management policy.
- In protecting its information assets, all parties shall comply with all applicable laws and regulations and requires its employees, contractors and agents to meet the highest ethical standards in dealing with all interested parties.
- All parties shall at all times, when processing, storing and transmitting Personal Information comply with the conditions as stipulated in POPIA. All systems that process, store or transmit Personal Information shall ensure that the integrity and confidentiality of the Personal Information is maintained at all times. The mechanisms selected to implement the integrity and confidentiality security services required by POPIA should comply with the Enterprise Security Architecture (ESA).

Physical security to Personal Information

- Access control and visitor management systems implemented for all visitors/guests.
- CCTV surveillance to protect restricted area.
- Locked cabinets for where paper files are stored.

Security to Personal Information

- The connection of unauthorised equipment to the Responsible Party's corporate LAN is prohibited. Authorisation must be obtained from the Responsible Party's Technology Security Officer with detailed motivations attached outlining the reason for the equipment to be connected.
- All servers, workstations, personal devices used to access the Operator's information resources, where technically possible, shall be loaded and protected with the latest approved anti-virus software.
- All servers, workstations, personal devices used to access the Operator's information resources, where technically possible, shall be password protected.
- Encryption technologies, where technically possible, shall be used to encrypt classified data stored on any device used to access the Operator's information resources.
- Recognising that some information is intended for specific individuals and shall not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages.
- Firewall policy management tools should be in place to protect against unauthorized electronic access to the Operator's network and to allow the Operator to track and monitor the flow of applications and important services over all areas of the network.
- All parties' firewalls must log all reports on daily, weekly, and monthly basis to allow the analysis of the network activity through the firewall.

- All incidents related to possible breach or compromise in information resources shall be escalated to the Operator's Information Officer\Privacy Officer and the Technology Security Officer.

Access control to Personal Information

- All service accounts shall be managed in accordance with the Operator's password policy.
- Users shall have a unique username and password to identify them on the various systems. All usernames and passwords shall conform to the approved naming and password conventions used by the Operator.
- Authorised users are responsible for the security of their passwords.
- Employees are given access on a need-to-know basis.
- All access logging and control to Personal Information should be recorded.
- Access to the systems and data shall be immediately terminated as soon as evidence of non-compliance with the security requirements are observed.