

OPERATOR AGREEMENT FOR THE PROTECTION OF PERSONAL INFORMATION

Between

ESKOM HOLDINGS SOC LTD

and

[DRAFTING NOTE: INSERT NAME OF COUNTERPARTY COMPANY]

This document contains confidential and proprietary information of Eskom and is “Eskom Confidential Information” for the purposes of the non-disclosure agreement entered into between Eskom and Supplier in relation to this Project. It is furnished for contract evaluation and award purposes only. Except with the express prior written permission of Eskom, this document and the information contained herein may not be published, disclosed, or used for any other purpose.

INSTRUCTIONS FOR RESPONDING TO THIS DOCUMENT:

General Guidelines

- These RFP documents contain the key legal terms and conditions that the Supplier will be required to comply with in relation to this Project.
- Eskom requires the Supplier to comply with the requirements as written, and compliance with these RFP documents will be a critical component of Supplier’s response to the RFP.
- The Supplier must complete Schedule Q (Supplementary Terms), as it is a mandatory requirement. Non-compliance will result in the Supplier being disqualified from further evaluation.

THIS AGREEMENT will be entered into by and between:

Eskom Holdings SOC Ltd, a company incorporated in South Africa with registered number 2002/015527/30 and having its registered office at Megawatt Park, Maxwell Drive, Sunninghill, Sandton ("**Eskom**"); and

[■] [**Drafting note: the Supplier to insert**], a company incorporated in [■] [**Drafting note: the Supplier to insert**] with registered number [■] [**Drafting note: the Supplier to insert**] and having its registered office at [■] [**Drafting note: the Supplier to insert**] ("**the Supplier**").

1. **INTERPRETATION**

In this Agreement:

- 1.1. clause headings are for convenience and are not to be used in its interpretation;
- 1.2. unless the context indicates a contrary intention, an expression which denotes any gender includes the other genders; a natural person includes a juristic person and vice versa; and the singular includes the plural and vice versa;
- 1.3. words and expressions defined in any clause shall, for the purposes of that clause, bear the meanings assigned to such words and expressions in such clause; and
- 1.4. if any provision is a substantive provision conferring rights or imposing obligations on any Party, notwithstanding that it is only in a definitions clause, effect will be given to it as if it were a substantive provision in the body of this Agreement;
- 1.5. the following expressions bear the meanings assigned to them below and cognate expressions bear corresponding meanings:
 - 1.5.1. "**Agreement**" means this agreement relating to the Protection of Personal Information;
 - 1.5.2. "**Customer**" means Eskom Holdings SOC Ltd;
 - 1.5.3. "**Confidential Information**" means, in respect of a Party, information in any form (whether written, electronic, graphic, oral, or otherwise) that falls within any of the following categories:
 - 1.5.3.1. Confidential or proprietary information provided by the Party (whether or not marked confidential (or a similar designation) or stated to be confidential at the time of disclosure;

- 1.5.3.2. it concerns the customers, finances, sales, marketing, products, suppliers, employees, business operations, forecasts, or management of, or it would ordinarily be deemed by a reasonable person to be confidential or proprietary to:
 - 1.5.3.2.1. in the case of Eskom Confidential Information: Service Recipients and the other Eskom Affiliates; or
 - 1.5.3.2.2. in the case of the Supplier Confidential Information: Supplier, the Subcontractors and the other the Supplier Affiliates;
- 1.5.3.3. information contained in, or relating to, the items licensed to the other Party pursuant to the Terms and Conditions;
- 1.5.3.4. information identified in the Agreement as Confidential Information of a Party; or
- 1.5.3.5. in the case of Eskom Confidential Information, information contained in the following:
 - 1.5.3.5.1. Eskom Data, Eskom Policies, and the Operations Manual; and
 - 1.5.3.5.2. any of the materials provided by either Party to the other Party that contains information about Eskom or its customers (including Eskom know how and trade secrets);
- 1.5.4. **“Data Subjects”** means the Customer's affiliates, customers, Staff, and any other Person/s to whom Personal Information relates;
- 1.5.5. **“Disclosing Party”** means the Party disclosing Personal Information relating to Data Subjects, irrespective as to whether this Party is the Supplier or the Customer;
- 1.5.6. **“Commencement Date”** means [Drafting Note: to be inserted] notwithstanding the signature hereof;
- 1.5.7. **“Electronic Communication”** means any text, voice, sound, or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until the recipient collects it;
- 1.5.8. **“Eskom Executive”** means the Eskom Chief Technology and Information Officer or his/her duly authorised representative;

- 1.5.9. **“Operator”** means a person who processes Personal Information for the Responsible Party in terms of a contract or mandate, without coming under the direct authority of the Responsible Party;
- 1.5.10. **“Parties”** mean the Parties to this Agreement being:
- 1.5.10.1. the Customer; and
 - 1.5.10.2. the Supplier;
- 1.5.11. **“Person”** means an identifiable living natural or existing juristic person or any other person who is not a natural or juristic person;
- 1.5.12. **“Personal Information”** means information relating to any Person, including but not limited to information relating to such Person’s:
- 1.5.12.1. race, sex, gender, sexual orientation, pregnancy, marital status, nationality, ethnic or social origin, colour, age, physical or mental health, well-being, disability, religion, conscience, belief, cultural affiliation, language, and birth;
 - 1.5.12.2. education, medical, financial, criminal or employment history;
 - 1.5.12.3. any identifying number, account or client number, password, pin code, customer or Data Subject code or number, numeric, alpha, or alpha-numeric design or configuration of any nature, symbol, e-mail address, domain name or IP address, physical address, cellular phone number, telephone number, or other particular assignment;
 - 1.5.12.4. blood type, fingerprint, or any other biometric information;
 - 1.5.12.5. personal opinions, views, or preferences;
 - 1.5.12.6. correspondence that is implicitly or expressly of a personal, private, or confidential nature (or further correspondence that would reveal the contents of the original correspondence);
 - 1.5.12.7. views or opinions of another individual about the Person;
 - 1.5.12.8. the name of the Data Subject, if it appears with other Personal Information relating to such Person, or if the disclosure of the name itself would reveal information about the Person;

- 1.5.12.9. all information linked to any juristic person, including details relating to its corporate structure, composition, and business operations irrespective of whether such information is in the public domain or not.
- 1.5.13. **“Processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including:
- 1.5.13.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, system testing, or use;
- 1.5.13.2. dissemination by means of transmission, distribution or making available in any other form by Electronic Communications or other means; or
- 1.5.13.3. merging, linking, blocking, degradation, erasure, or destruction;
- 1.5.13.4. and “Process” has a corresponding meaning;
- 1.5.14. **“Information Regulator”** means information regulator as defined in *the Protection of Personal Information Act, 2013*;
- 1.5.15. **“Relationship”** means the ongoing relationship between the Parties relating to, inter alia, the provision of research, products, and/or services by the Supplier to the Customer whether provided in terms of Services Agreements or otherwise;
- 1.5.16. **“Responsible Party”** means the person who, alone or in conjunction with others, determines the purpose of and means for processing Personal Information, and who is also the Customer;
- 1.5.17. **“Receiving Party”** means the Party, other than the Disclosing Party, which receives disclosure of any of the Confidential Information or Personal Information relating to Data Subjects, as determined by the context;
- 1.5.18. **“Services Agreement(s)”** means all services or supply agreement/s which are entered into between the Parties from time to time **[Drafting note: Insert details of underlying contract for instance, NEC or bespoke]**;
- 1.5.19. **“Security Standards”** means the security standards protocol, a copy of which is attached hereto, alternatively a copy was handed to the Supplier by the Customer and which the Supplier acknowledges to be bound by; **[Drafting note: Include Eskom Security Standard/Policy]**
- 1.5.20. **“Staff”** means permanent, fixed term and temporary employees as well as subcontractors, agents, consultants, independent contractors and visiting students

to the Supplier and Customer who process Personal Information on behalf of the Supplier or Customer, as applicable; and

- 1.5.21. **“Supplier”** means the entity as defined on the first page hereof, that may also be fulfilling functions as an Operator.

2. **RECORDAL**

- 2.1. The Parties have engaged, or are about to engage, in a Relationship.
- 2.2. In the course of the Relationship and in any future interactions between the Parties, there is a likelihood that the Supplier will receive, be exposed to and/or Process the Personal Information of the Data Subjects.
- 2.3. The Supplier recognises that the Data Subjects and the Customer may suffer irreparable harm or loss in the event of the Personal Information being processed otherwise than in accordance with this Agreement.

3. **COMMENCEMENT DATE AND TERM**

- 3.1. The Supplier agrees that the terms and conditions of this Agreement shall apply as of the Commencement Date.
- 3.2. The obligations of the Supplier as set forth herein shall endure for an indefinite period from receipt of any Personal Information and shall apply in respect of all Services Agreements entered into between the Parties, it being agreed that the terms of this Agreement shall prevail over any terms set forth in such Services Agreements which relate to the subject matter of this Agreement save to the extent that any such Services Agreement explicitly seeks to supplement or amend the terms of this Agreement.

4. **OBLIGATIONS OF THE SUPPLIER WITH RESPECT TO PERSONAL INFORMATION**

- 4.1. The Supplier shall:
- 4.1.1. only Process Personal Information in accordance with Applicable Laws, in terms of this Agreement and in accordance with any instructions, requirements or specific directions of the Customer;
- 4.1.2. comply with the requirements set forth in the Security Standards and in all other Customer policies provided by the Customer in ~~ts~~ regard. The Customer will advise the Supplier of any amendments to the Security Standards and any policies applicable to it;

- 4.1.3. treat the Personal Information as strictly confidential;
- 4.1.4. not disclose or otherwise make available the Personal Information to any third party (including sub-contractors and Staff) other than authorised Staff who require access to such Personal Information strictly in order for the Supplier to carry out its obligations pursuant to the Relationship, unless the Customer has provided its prior written permission to do so to the Supplier, and the Supplier has submitted a copy of a written contract to the Customer, to the satisfaction of the Customer, that the Supplier has entered into with a third party for the protection of Personal Information of the Data Subjects;
- 4.1.5. ensure that all Staff and any other persons that have access to the Personal Information are bound by appropriate and legally binding confidentiality and non-use obligations in relation to the Personal Information on substantially the same terms and conditions as set forth in the Non-Disclosure Agreement;
- 4.1.6. take appropriate, reasonable technical and organisational measures to ensure that the integrity of the Personal Information in its possession or under its control is secure and that such Personal Information is protected against unauthorised or unlawful processing, accidental loss, destruction or damage, alteration, disclosure, or access by:
 - 4.1.6.1. having regard to:
 - 4.1.6.1.1. any requirement set forth in law, stipulated in industry rules or in codes of conduct or by a professional body; and
 - 4.1.6.1.2. generally accepted information security practices and procedures which apply to (i) the Supplier's business; and (ii) to the Customer;
 - 4.1.6.2. identifying all reasonably foreseeable internal and external risks and, at least once in every 12 (twelve)-month period and, subject to the provisions of clauses 4.1.6 and 10, take all necessary steps at its own cost to:
 - 4.1.6.2.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control and provide the Customer with a detailed written report using generally accepted auditing methodologies, within

30 (thirty) days of having completed its investigations, regardless as to whether the frequency of such investigations is 12 (twelve) monthly or more frequently;

4.1.6.2.2. with the Customer's prior written approval, implement and maintain appropriate safeguards against the risks identified by the Supplier;

4.1.6.2.3. regularly verify that the safeguards which the Supplier has in place have been effectively implemented and provide the Customer with a written report within 30 (thirty) days of having completed each such verification exercise; and

4.1.6.2.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards, with all upgrades, which may have an impact on any Personal Information within the possession of the Supplier as a result of the Relationship, to be reported to the Customer in writing;

4.1.6.3. complying with the auditing requirements set forth in this Agreement; and

4.1.6.4. agreeing to reasonable amendments to this Agreement from time to time, to the extent that data protection legislation or the law generally requires such amendments for the benefit of Data Subjects.

4.1.7. The Supplier shall comply, at all times, with the Customer's Information Security policies, including Schedule R (Information Security Requirements), and ensure that all Processing activities are consistent with the requirements of the Protection of Personal Information Act 4 of 2013, as amended, and any regulations published thereunder.

5. NOTIFICATION OF A PERSONAL INFORMATION SECURITY BREACH

5.1. The Supplier shall

5.1.1. notify the Eskom Executive of the Customer in writing, at **Drafting note: email address to be inserted, (Contracts Advisor, Name of information security**

team member at infosecurity@eskom.co.za immediately, if possible, but no later than 48 (forty-eight) hours of the Supplier becoming aware of or suspecting any unauthorised or unlawful use, disclosure or processing of Personal Information and comply with the following –

- 5.1.1.1. at its own cost, take all necessary steps to mitigate the extent of the loss or compromise of Personal Information and to restore the integrity of the affected information systems as quickly as possible;
- 5.1.1.2. furnish the Customer with details of the Data Subjects affected by the compromise and the nature and extent of the compromise, and if known, include details of the identity of the unauthorised person who may have accessed or acquired the Personal Information;
- 5.1.1.3. provide the Customer through its Eskom Executive with a report on its progress in resolving the compromise at reasonable intervals but at least once per business day following the initial notification to the Customer, until such time as the compromise is resolved to the Customer's satisfaction;
- 5.1.1.4. in consultation with the Customer and where required by law notify the South African Police Service; and/or the National Intelligence Agency;
- 5.1.1.5. only upon request by the Customer, or otherwise if required by law, notify the Information Regulator and/or the affected Data Subjects. Any such notification shall be in a form prescribed by the Customer or the Information Regulator, as the case may be, if applicable, and contain such information as is specified by the Customer and or the Information Regulator. Notwithstanding the foregoing, a notification to a Data Subject shall always include sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise;
- 5.1.1.6. assist the Customer to comply with any requests for access to Personal Information received by the Customer from Data Subjects and, at the request of the Customer, the Supplier shall promptly provide the Customer with a copy of any Personal Information held by the Supplier in relation to a specified Data Subject;

- 5.1.1.7. The Supplier agrees that notwithstanding the confidentiality provisions of this Agreement, the Customer may disclose to a Data Subject that the Supplier has been or is involved in Processing such DataSubject's Personal Information;
- 5.1.1.8. provide reasonable evidence of the Supplier's compliance with its obligations under this clause 5 to the Customer on reasonable notice and request;
- 5.1.1.9. under instruction and authority of the Customer, and at no extra cost to the Customer, provide it with all assistance required for the Customer to discharge its duties as Responsible Party relating to a requirement by the Information Regulator (a) for the Customer as Responsible Party to submit an independent auditor's report or other information relating to interference by the Responsible Party with the Personal Information of a Data Subject, (b) that the Customer is processing Personal Information in accordance with legislation, or (c) that the Customer is otherwise compliant with any other relevant legislation;
- 5.1.1.10. at the request and option of the Customer, and to its satisfaction, promptly return or destroy all Personal Information in the possession or control of the Supplier, including in accordance with any specific retention, destruction and purging requirements as may be prescribed by the Customer; and
- 5.1.1.11. not Process the Personal Information other than in accordance with clause 6.

6. PERMITTED PROCESSING OF PERSONAL INFORMATION

6.1. The Supplier shall only Process the Personal Information of Data Subjects:

- 6.1.1. for a specific, lawful purpose strictly in accordance with the Customer's express written instructions through its Eskom Executive (as may be set forth in an annexure hereto or a Services Agreement) and shall not carry out any related or further processing activities for any other reason whatsoever (including any related processing functions or processing which would otherwise be a normal extension of the Processing which the Supplier is entitled to undertake in accordance with the Customer's instructions) without the express prior written consent of the Customer through its Eskom Executive, save that the Supplier

may carry out reasonable further Processing strictly in order to comply with an obligation which is imposed on it by law and in such circumstances, the provisions of clause 7 shall apply;

- 6.1.2. in a manner that does not infringe the privacy of the Data Subject, in accordance with relevant legislation relating to the Processing of Personal Information; and
- 6.1.3. subject to the provisions of this clause 6 and the provisions of the Promotion of Access to Information Act 2 of 2002, by engaging and communicating solely with the Customer, and is not permitted to disclose to any Data Subject that it is Processing, has Processed or intends to Process the Personal Information of such Data Subject unless it has obtained the prior written consent of the Customer through its Eskom Executive in this regard.

7. DISCLOSURE OR PROCESSING REQUIRED BY LAW, REGULATION OR COURT ORDER

7.1. In the event that the Supplier is required to disclose or Process any Personal Information required by law, regulation or court order, or if the Processing of such Personal Information is required to enable a public body to properly perform a public law duty to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party, is necessary for pursuing the legitimate interests of the Customer, a third-party to whom the information is supplied, or a Data Subject, or complies with an obligation imposed by law on the Customer, the Supplier

- 7.1.1. will advise the Customer thereof prior to disclosure, if possible. If prior disclosure is not possible, the Supplier shall advise the Customer immediately after such disclosure;
- 7.1.2. will take such steps to limit the extent of the disclosure or Processing as far as it reasonably practically and legally can;
- 7.1.3. will afford the Customer a reasonable opportunity, if possible and permitted, to intervene in the proceedings; and
- 7.1.4. will comply with the Customer's requests as to the manner and terms of any such disclosure or Processing, if possible and permitted.

8. SEPARATION OF PERSONAL INFORMATION

Unless otherwise specifically recorded in this Agreement or any other agreement concluded between the Parties, any Processing of Personal Information shall be conducted separately from Personal Information, data and property relating to the Supplier or any third party and may not be combined or

merged with information of another party unless such combination or merging takes place for credit vetting purposes or as instructed in writing by Eskom.

9. **TRANSFER OF PERSONAL INFORMATION**

9.1. The Supplier shall ensure that no Personal Information is transferred outside of the Republic of South Africa unless –

- 9.1.1. the Customer provides its prior written consent to the transfer;
- 9.1.2. the recipient is subject to a law, code of conduct or contract which provides comparable protection for the Personal Information as the protections contained in this Agreement, including similar provisions relating to the further transfer of the Personal Information;
- 9.1.3. the transfer is necessary for the performance of a contract between the Data Subject and the Customer, or a contract between the Customer and the Supplier which is in the interest of the Data Subject; or
- 9.1.4. the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.
- 9.1.5. Any Processing of Personal Information in cloud environments or outside the Republic of South Africa must also comply with protection standards recognised under POPIA.

9.2. Even in circumstances where the Customer has consented to any such cross-border transfer, the Supplier agrees to comply strictly with the Customer's express instructions for such cross-border transfers including as it may be set forth in any annexure hereto or in the relevant Services Agreement.

10. **AUDIT RIGHTS OF THE CUSTOMER**

10.1. The Customer or its agent shall have the right to audit the Supplier at any time, with reasonable notice, in order to determine whether the Supplier complies with the terms and conditions of this Agreement with regard to the protection of Personal Information and the security exercised by the Supplier relating thereto. Such audit rights shall include but not be limited to the right of access to systems, procedures and software, and inspection of the physical security of the Supplier's premises. The Supplier shall offer reasonable assistance and co-operation to the Customer and/or its auditors or inspectors in the carrying out of such auditing exercise.

- 10.2. To the extent that the Supplier engages an independent auditor in relation to the provisions of applicable data protection legislation to carry out an audit of its operations, the Supplier agrees to provide the Customer with copies of the audit reports of all such audit exercises.
- 10.3. Should any audit exercise reveal any non-compliance with the terms of this Agreement, the Security Standards or any other Customer policies, the Supplier shall be required to take all necessary steps to rectify such non-compliance immediately.
- 10.4. The Customer may at any time during the term of this Agreement, at its sole discretion, elect to waive, in full or in part, its right to conduct an audit in respect of the Supplier's compliance with the security requirements, business continuity requirements, or disaster recovery requirements, where the Supplier furnishes the Customer with independent third party certifications, such as but not limited to SOC 2 Type II reports, ISO/IEC 27001 certifications, NIST certification, or similar certifications.

11. CONFIDENTIALITY

- 11.1. **Acknowledgement of importance of Confidential information:** The Receiving Party acknowledges the great importance of the Confidential Information to the Disclosing Party and, where applicable, third-party proprietors of such information, and recognises that the Disclosing Party and/or third-party proprietors may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Agreement.
- 11.2. **Receiving Party's undertaking:** The Receiving Party agrees and undertakes –
- 11.2.1. **No publication of Confidential Information:** 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 Disclosing Party and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Receiving Party to obtain the consent of such third party;
- 11.2.2. **No exploitation of Confidential Information:** 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 Disclosing Party and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Receiving Party to obtain the consent of such third party;
- 11.2.3. **Restricting dissemination of Confidential Information:** 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 Receiving Party shall initiate, maintain and monitor internal security procedures reasonably acceptable to the Disclosing Party to prevent unauthorised disclosure by its Staff; and

- 11.2.4. **Obligations with regard to Staff:** 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.
- 11.3. **Further acknowledgements:** All Confidential Information disclosed by the Disclosing Party to the Receiving Party or which otherwise comes to the knowledge of the Receiving Party, is acknowledged by the Receiving Party –
- 11.4. Confidential **Information is proprietary:** to be proprietary to the Disclosing Party.
- 11.5. **Standard of care:** The Receiving Party shall protect the Confidential Information in the manner, and with the endeavour, of a reasonable person protecting his/her own Confidential Information. In no event shall the Receiving Party use less than reasonable efforts to protect the confidentiality of the Confidential Information.
- 11.6. **Return of Confidential Information:** The Disclosing Party may at any time on written request to the Receiving Party, require that the Receiving Party immediately return to the Disclosing Party any Confidential Information and may, in addition, require that the Receiving Party 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 Confidential Information or material. Alternatively, the Receiving Party shall, as and when required by the Disclosing Party on written request to the Receiving Party, destroy all such Confidential Information and material and furnish the Disclosing Party with a written statement to the effect that the same has been destroyed. The Receiving Party shall comply with any request in terms of this clause 11.5 within 7 (seven) days of receipt of such request.
- 11.7. **Retention of Confidential Information:** The Supplier may retain Confidential Information to the extent required by, and for the duration of, any Services performed for the Customer in terms of agreements between the Parties, provided that the Customer has not waived performance of such Services and subject to the right of the Customer to recover the Confidential Information at any time in terms of clause 11.5.
- 11.8. **Procure undertakings from Staff:** The Supplier shall procure that the Supplier’s Staff who have access to Confidential Information, give a written undertaking in favour of the Customer in regard to the Confidential Information on substantially the same terms and conditions contained

within this Agreement in a form prescribed by the Customer. The Customer shall be entitled to deny a Supplier Staff member access to its premises or prevent such member conducting any work in relation to the Services or under the Customer's direct control, should the Customer not be in receipt of a signed undertaking from such member on such terms and conditions as determined by the Customer. The Customer's failure to obtain receipt of the undertaking referred to in this clause 11.7 shall in no way detract from the Supplier's obligations in terms of this Agreement.

11.9. **Exceptions to this clause 11:** Clause 11 shall not be applicable where the Receiving Party discloses Confidential Information to attorneys or auditors, provided that such disclosure is reasonably required by the Receiving Party for the purposes of conducting its business activities.

11.10. **Disclosure required by law, regulation, or court order:** In the event that the Receiving Party is required to disclose the Confidential Information, the Receiving Party –

11.10.1. will advise the Disclosing Party thereof prior to disclosure, if possible;

11.10.2. will take such steps to limit the extent of the disclosure to the extent that it lawfully and reasonably practically can;

11.10.3. will afford the Disclosing Party a reasonable opportunity, if possible, to intervene in the proceedings; and

11.10.4. will comply with the Disclosing Party's requests as to the manner and terms of any such disclosure.

11.11. **Obligations in terms of this clause:** The obligations of the Receiving Party 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 11 shall endure notwithstanding any termination of this Agreement, any other agreement entered into between the Parties or any discussions between the Parties.

12. **PERSONAL INFORMATION INDEMNITY**

12.1. The Supplier hereby indemnifies and holds harmless the Customer and its staff, successors, cessionaries delegates and assigns, from any and all losses of a patrimonial and non-patrimonial nature, costs, expenses and damage, including consequential losses and damage as well as penalties and fines arising from the Supplier's non-compliance with the provisions of any relevant legislation applicable to Personal Information/data protection, as well as damage to the Customer's reputation and costs of compliance as directed by the Information

Regulator, including but not limited to publication of the data breach and call centre costs for support to affected Data Subjects.

13. SUBCONTRACTORS

The Supplier acknowledges and agrees that:

- 13.1. it may not sub-contract its obligations under this Agreement without the prior written consent of the Customer;
- 13.2. the Customer has the right to audit any sub-contractor to ensure that it is capable of complying with the obligations imposed with respect to the Protection of Personal Information; and
- 13.3. the provisions of this Agreement shall mutatis mutandis apply to all subcontractors authorised by the Customer who process Personal Information of Data Subjects.

14. RETENTION AND DESTRUCTION REQUIREMENTS

- 14.1. The Supplier shall be required to comply with the destruction and retention policies of the Customer as are either set forth in Services Agreements or in the Security Standards or as may be communicated to the Supplier. In particular, the Supplier shall store all Personal Information which it Processes for the minimum time periods as are stipulated by the Customer in the aforementioned policies and shall be required to destroy all Personal Information relating to the Data Subjects in compliance with the destruction time periods stipulated in the aforementioned policies and in accordance with the Customer's specified destruction procedures and methodology.
- 14.2. Should any destruction instructions not be specified in a Services Agreement or in the Security Standards when the Services Agreement in terms of which any Personal Information has been Processed by the Supplier terminates or expires, the Supplier shall be required to timeously obtain written instructions from the Customer for the return and/or destruction of all such Personal Information in its possession.

15. TRANSMISSION OF DATA

The Supplier shall ensure that all Personal Information communicated, including, without limitation, any digital communication or any Personal Information stored in digital form shall be secured against being accessed or read by unauthorised parties, using appropriate security safeguards, having due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

16. APPLICABLE LAW

This Agreement shall be governed by and construed in accordance with the law of the Republic of South Africa and all disputes, actions and other matters relating thereto shall be determined in accordance with such law.

17. JURISDICTION

17.1. The Supplier consents and submits to the jurisdiction of the South Gauteng High Court in any dispute arising from or in connection with this Agreement.

17.2. Without prejudice to any other rights or remedies which the Customer may have, the Supplier acknowledges that nothing herein shall preclude the Customer from seeking urgent relief or specific performance from a court of competent jurisdiction.

18. NOTICES AND DOMICILIUM

18.1. The Supplier selects as its *domicilium citandi et executandi* the physical address appearing on the first page, and for the purposes of giving or sending any notice provided for or required hereunder, the address and telefax number appearing on the first page or such other addresses or telefax number as may be substituted by notice given as herein required.

18.2. The Supplier acknowledges that any notice it sends to Customer relating to this Agreement shall be marked for the attention of [Drafting note: Name : the Contract Advisor]; and shall be delivered to the Customer at its *domicilium citandi et executandi*, being [Drafting note: to be inserted Eskom Address/ email] and for the purpose of giving or sending any notice provided for or required, or such other addresses or telefax number as may be substituted by notice given by the Customer to the Supplier.

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

18.2.2. Any notice shall be deemed to have been given and received –

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

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

18.2.2.3. if sent by telefax on the date of sending of such telefax, unless the contrary is proven, provided that such notice shall be confirmed by prepaid registered post on the date of dispatch of such telefax or,

should no postal facilities be available on that date, on the next business day.

18.3. Notwithstanding anything to the contrary contained in this clause 18, 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 18.2.

19. **WHOLE AGREEMENT**

19.1. Subject to clause 3.2, 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.

19.2. No addition to, variation, consensual cancellation or novation of this Agreement shall be of any force or effect unless reduced to writing and signed by both Parties.

20. **ASSIGNMENT**

The Supplier shall not be entitled to assign or otherwise transfer the rights and obligations of all or any part of this Agreement without the prior written consent of the Customer.

21. **WAIVER**

No waiver of any of the terms and conditions of this Agreement will be binding or effectual for any purpose unless expressed in writing and signed by the Customer giving same, and any such waiver will be effective only in the specific instance and for the purpose given. No failure or delay on the part of the Customer in exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise of any right, power or privilege preclude any other or further exercise thereof or the exercise of any other right, power or privilege.

22. **SEVERABILITY**

Should any of the terms and conditions of this Agreement be held to be invalid, unlawful, or unenforceable, such terms and conditions will be severable from the remaining terms and conditions which will continue to be valid and enforceable. If any term or condition held to be invalid is capable of amendment to render it valid, the Parties agree to enter into negotiations to resolve the invalidity.

23. **COSTS**

Each Party shall bear and pay its own costs of or incidental to the drafting, preparation, and execution of this Agreement.

Signed at Sandton, Megawatt Park on behalf of _____ on this _____ day
of _____ 202_ in the presence of the undersigned witnesses, by:

who is duly authorised to sign in his/her capacity as

Witnesses:

1 Name _____ Signature: _____

2 Name _____ Signature: _____

Signed at Sandton, Megawatt Park on behalf of _____ on this _____ day
of _____ 202_ in the presence of the undersigned witnesses, by:

Name: _____

Signature: _____

who is duly authorised to sign in his/her capacity as

Witnesses:

1 Name _____ Signature: _____

2 Name _____ Signature: _____