MCi DATA PROCESSING AGREEMENT

1. INTRODUCTION

1.1 **MCi Consultants (Pty) Ltd. ('MCi')** is a leading software and services provider. **MCi** provides products and services ('Services') to the Client under the **Agreement ('The Client Agreement')**.

1.2 To the extent **MCi** may be required to process personal information on behalf of the Client under the **Client Agreement**, **MCi** will do so in accordance with the terms set out in this **Data Processing Agreement ('DPA')**.

2. DEFINED TERMS

2.1 '**Data Protection Laws**' means any law relating to data protection privacy, and security applicable to a party in connection with the processing of personal information under **the Client Agreement** including but not limited to (each as amended or replaced from time to time) (a) POPIA, and (b) **any applicable laws worldwide** relevant to **MCi** or the Client (where applicable and as recipient of services provided by **MCi**) relating to data protection.

2.2 '**Personal information**' means all personal information provided to **MCi** by, or on behalf of, the Client through **MCi's** provision of the Services.

2.3 '**Data Privacy and Protection Agreement'** means the then-current **Data Privacy and Protection Agreement** describing **MCi's** treatment of personal information in its general business administration, management, and operations, which is made available at https://www.mci.co.za/legal and as may be updated by **MCi** from time-to-time (effective upon publication).

2.4 '**POPIA**' means the Protection of Personal Information Act 4 of 2013.

2.5 **Lower case terms:** The following lower-case terms used but not defined in this DPA, such as '**data subject**', '**information regulator**', '**operator**', '**personal information**', '**responsible party**' and '**processing**' will have the same meaning as set forth in section 1 of POPIA, or where not specifically defined under Data Protection Laws, the same meaning as analogous terms in those Data Protection Laws.

3. APPLICABLE LAW

3.1 **MCi** may be required to process personal information on behalf of the Client under any applicable Data Protection Laws.

3.2 Unless expressly stated otherwise, in the event of any conflict between the main body of this DPA and Data Protection Laws, the applicable Data Protection Laws will prevail.

4. DURATION AND TERMINATION

4.1 This DPA will commence on the date as the **Client Agreement** is signed by the party who signs it last and will remain in force so long as the **Client Agreement** remains in effect or **MCi** retains any personal information related to the **Client Agreement** in its possession or control.

4.2 **MCi** will process personal information until the date of expiration or termination of the **Client Agreement**, unless instructed otherwise by the Client in writing, or until such personal information is returned or destroyed on the written instructions of the Client or to the extent that **MCi** is required to retain such personal information to comply with applicable laws.

5. PERSONAL INFORMATION TYPES AND PROCESSING PURPOSES

5.1 The Client and **MCi** acknowledge that the Client is the responsible party and **MCi** is the operator or sub-operator of personal information.

5.2 The details of the processing operations, in particular the categories of personal information and the purposes of processing for which the personal information is processed on behalf of the responsible party concerning the Services described in the **Client Agreement**, are specified in **Clause 18**.

5.3 The Client remains responsible for its compliance obligations under applicable Data Protection Laws, including providing any required notices, obtaining any required consents, and for the processing instructions it gives to **MCi**.

6. MCi OBLIGATIONS

6.1 **Client knowledge, authorisation and documented instructions**. When MCi acts as the operator of personal information, it will only process the personal information with the Client's knowledge, authorisation, and on the Client's documented instructions as identified in **Clause 18**, and to the extent that this is required to fulfil the Services as per the **Client Agreement**. MCi will not process the personal information for any other purpose or in a way that does not comply with this DPA or applicable Data Protection Laws.

6.2 **Processing beyond instructions.** Should MCi reasonably believe that a specific processing activity beyond the scope of the Client's instructions is required to comply with a legal obligation to which MCi is subject, MCi must inform the Client of that legal obligation and seek explicit authorisation from the Client before undertaking such processing. MCi will not process the personal information in a manner inconsistent with the Client's documented instructions.

6.3 **Independent responsible party**. To the extent MCi uses or otherwise processes personal information in connection with **MCi's** legitimate business operations, MCi will be an independent responsible party for such use, will process personal information in accordance with its **Data Privacy and Protection Agreement**, and will be responsible for complying with all applicable laws and responsible party obligations.

6.4 **Compliance**. MCi will reasonably assist the Client in complying with the Client's obligations under applicable Data Protection Laws, considering:

6.4.1 the nature of **MCi's** processing,

6.4.2 the information made available to **MCi,** including in relation to data subject rights,

6.4.3 data protection impact assessments and

6.4.4 reporting to and consulting with information regulator.

6.5 **Notification.** MCi will immediately notify the Client if, in its opinion, any instruction infringes applicable Data Protection Laws. This notification will neither constitute a general obligation on the part of MCi to monitor or interpret the laws applicable to the Client, nor constitute legal advice to the Client.

6.6 **Disclosure**. MCi will not disclose personal information except: (a) as the Client directs in writing, (b) as described in this DPA or (c) as MCi will use reasonable endeavors to notify the Client and attempt to redirect the public authority to request the personal information directly from the Client.

7. CONTRACTING WITH SUB-OPERATORS

7.1 **List of sub-operators**. A list of **MCi's** sub-operators that MCi directly engages for the specific Services as an operator is available on request to the MCi contact mentioned in Clause 17**.**

7.2 **General authorisation.** The Client provides its general authorisation to **MCi's** engagement with sub-operators, to provide some of Services e.g. hosting services, on its behalf. To the fullest extent permissible under applicable Data Protection Laws this DPA will constitute the Client's general written authorisation to the sub-contracting by MCi of the Services as disclosed to the Client.

7.3 **Changes.** MCi will notify the Client in writing of any intended changes to the agreed outsourced Services.

7.4 **Performance**. MCi is responsible for its sub-operator's compliance in relation to **MCi's** obligations in this DPA.

8. THE CLIENT OBLIGATIONS

8.1 **Data Subject requests**. If MCi receives a request from the Client's data subject to exercise one or more of its rights under applicable Data Protection Laws, in connection with a Service for which MCi is an operator, MCi will redirect the data subject to make its request directly to the Client. The Client will be responsible for responding to any such request. MCi will comply with reasonable requests by the Client to assist with the Client's response to such a data subject request. The Client will be responsible for reasonable costs MCi incurs in providing this assistance.

8.2 **The Client requests**. MCi must promptly comply with any Client request (a) requiring MCi to amend, transfer, delete or otherwise process the personal information, or to stop, mitigate or remedy any unauthorised processing, (b) relating to the Client's obligations regarding the security of processing and (c) the Client's obligations in terms of applicable Data Protection Laws, considering the nature of the processing and the information available to MCi.

8.3 **Warranty**. The Client warrants that: (a) it has all necessary rights to provide the personal information to **MCi** for the processing to be performed in relation to the Services, and (b) **MCi's** expected use of the personal information for the Services as specifically instructed by the Client, will comply with all applicable Data Protection Laws.

8.4 **Privacy notices**. To the extent required by applicable Data Protection Laws, the Client is responsible for ensuring that all necessary privacy notices are provided to data subjects, and unless another legal basis set forth in applicable Data Protection Laws supports the lawfulness of the processing, any necessary data subject consents to the processing are obtained and a record of such consents is maintained. Should such consent be revoked by a data subject, the Client is responsible for communicating the fact of such revocation to **MCi**, and **MCi** remains responsible for implementing the Client's instruction with respect to the processing of that personal information.

9. SECURITY

9.1 **TOMs**. **MCi** will implement appropriate and reasonable **Technical and Organisational Measures** ('**TOMs**') to ensure the security of the personal information in terms of applicable Data Protection Laws, including the security measures set out in Clause 19. This includes protecting the personal information against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the personal information.

9.2 **Access to personal information. MCi** will grant access to the personal information undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring the **Client Agreement**. **MCi** will ensure that persons authorised to process the personal information received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10. AUDITS

10.1 **Certifications**. **MCi** will maintain any certifications that it is contractually obligated to maintain and comply with as expressly stated in the **Client Agreement**. **MCi** will re-certify against those certifications as reasonably required.

10.2 **Provision of evidence**. At the Client's written request, **MCi** will provide the Client with evidence of those certifications relating to the processing of personal information, including applicable certifications or audit reports of its computing environment and physical data centers that it uses in processing personal information to provide the Services so that the Client can reasonably verify the data centers compliance with its obligations under this DPA.

10.3 **Compliance with TOMS**. **MCi** may also rely on those certifications to demonstrate compliance with the requirements set out in clause 9.1.

10.4 **Confidential information**. Any evidence provided by **MCi** is confidential information and is subject to non-disclosure and distribution limitations of **MCi** and/or any **MCi** sub-operator.

10.5 **The Client Audits**. The Client may carry out audits of **MCi´s** premises and operations as these relate to the personal information of the Client if:

10.5.1 **MCi** has not provided sufficient evidence of the measures taken under clause 9; or

10.5.2 an audit is formally required by the information regulator; or

10.5.3 applicable Data Protection Laws provide the Client with a direct audit right (and as long as the Client only conducts an audit once in any twelve-month period unless mandatory applicable Data Protection Laws require more frequent audits).

10.6 **The Client audit process**. The Client audit may be carried out by a third party (but must not be a competitor of **MCi** or not suitably qualified or independent) who must first enter into a confidentiality agreement with **MCi**. The Client must provide at least 60 days advance notice of any audit unless mandatory applicable Data Protection Laws or a data protection authority of competent jurisdiction requires shorter notice. **MCi** will cooperate with such audits carried out and will grant the Client´s auditors' reasonable access to any premises and devices involved with the processing of the Client's personal information. The Client audits will be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimise repetitive audits. The Client must bear the costs of any Client audit unless the audit reveals a material breach by **MCi** of this DPA in which case **MCi** will bear the costs of the audit. If the audit determines that **MCi** has breached its obligations under the DPA, **MCi** will promptly remedy the breach at its own cost.

11. INCIDENT MANAGEMENT

11.1 **Security incidents**. If **MCi** becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information while processed by **MCi** (each a '**Security Incident**'), **MCi** will promptly and without undue delay:

11.1.1 notify the Client of the Security Incident.

11.1.2 investigate the Security Incident and provide the Client with sufficient information about the Security Incident, including whether the Security Incident involves personal information of the Client.

11.1.3 take reasonable steps to mitigate the effects and minimise any damage resulting from the Security Incident.

11.2 **Security incident notification**. Notification(s) of Security Incidents will take place in accordance with clause 11.1. Where the Security Incident involves personal information of the Client, **MCi** will make reasonable efforts to enable the Client to perform a thorough investigation into the Security Incident, formulate a correct response, and take suitable further steps in respect of the Security Incident. **MCi** will make reasonable efforts to assist the Client in fulfilling the Client's obligation under section 22 of POPIA or other applicable Data Protection Laws to notify the relevant data protection authority and data subjects about such Security Incident. **MCi's** notification of or response to a Security Incident under this clause is not an acknowledgement by **MCi** of any fault or liability for the Security Incident.

11.3 **Other incidents**. **MCi** will notify the Client promptly if **MCi** becomes aware of:

11.3.1 a complaint or a request concerning the exercise of a data subject's rights under any applicable Data Protection Laws about personal information **MCi** processes on behalf of the Client and its data subjects; or

11.3.2 an investigation into or seizure of the personal information of the Client by government officials, or a specific indication that such an investigation or seizure is imminent; or

11.3.3 where, in the opinion of **MCi**, implementing an instruction received from the Client about the processing of personal information would violate applicable laws to which the Client or **MCi** are subject.

11.4 **The Client notifications.** Any notifications made to the Client under clause 11 will be addressed to the Client as per the **Client Agreement**.

12. CROSS BORDER TRANSFERS OF PERSONAL INFORMATION

12.1 **General.** Except as described elsewhere in the DPA, personal information that **MCi** processes on the Client's behalf may be transferred to and stored and processed in any country in which **MCi** or its sub-operators may operate.

12.2 **Adequate safeguards**. **MCi** will identify in Clause 18 the transfer mechanism that provides an appropriate level of protection to the third party who receives the personal information either by way of a law, binding corporate rules or binding agreement under section 72(1)(a) of POPIA.

13. RETURN OR DESTRUCTION OF PERSONAL INFORMATION

13.1 **The Client deletion.** For certain Services, **MCi** is responsible for installing, hosting, and processing personal information. Here only **MCi** can access, extract and delete personal information stored in that Service. Where the particular Service does not support access, retention or extraction of software provided by the Client, **MCi** has no liability for the deletion of personal information as described in this clause 13.1

13.2 **Delete or return**. Where the **Client Agreement** requires **MCi** to retain personal information, **MCi** will delete that personal information within the period agreed to in the **Client Agreement**, unless **MCi** is permitted or required by applicable law to retain such personal information. Where the retention of personal information has not been addressed in the **Client Agreement**, **MCi** will either delete, destroy, or return all personal information to the Client and destroy or return any existing copies when **MCi** has finished providing Services:

13.2.1 related to the processing.

13.2.2 when this DPA terminates.

13.2.3 The Client requests **MCi** to do so in writing; or

13.2.4 **MCi** has otherwise fulfilled all purposes agreed in the context of the Services related to the processing activities where the Client does not require **MCi** to do any further processing.

13.3 **Certificate of destruction**. **MCi** will provide the Client with a destruction certificate at the Client's request. Where the deletion or return of the personal information is impossible for any reason, or where backups and/or archived copies have been made of the personal information, **MCi** will retain such personal information in compliance with applicable Data Protection Laws.

13.4 **Third parties**. On termination of this DPA, **MCi** will notify all sub-operators supporting its processing and make sure that they either destroy the personal information or return the personal information to the Client, at the discretion of the Client.

14. LIABILITY AND WARRANTY

14.1 Any limitation of liability in the **Client Agreement** will apply to this DPA, other than to the extent such limitation (a) limits the liability of the parties to data subjects or (b) is not permitted by applicable law.

15. NOTICE

15.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to the other party by email.

15.2 Clause 15.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

15.3 Any notice or other communication will be deemed given when:

15.3.1 delivered in person.

15.3.2 received by mail (postage prepaid, registered or certified mail, return receipt requested); or

15.3.3 received by an internationally recognised courier service (proof of delivery received by the noticing party) at the physical notice address (as identified above), with an electronic copy sent to the electronic notice address (as identified in the table above).

16. MISCELLANEOUS

16.1 **Conflict of terms**. The **Client Agreement** terms remain in full force and effect except as modified in this DPA. Insofar as **MCi** will be processing personal information subject to applicable Data Protection Laws on behalf of the Client in the course of the performance of the **Client Agreement,** the terms of this DPA will apply. If the terms of this DPA conflict with the terms of the **Client Agreement**, the terms of this DPA will take precedence over the terms of the **Client Agreement**.

16.2 **Governing law**. This DPA is governed by South African law.

16.3 Subject to clause 16.4 (Dispute Resolution):

16.3.1 The Client irrevocably submits to the exclusive jurisdiction of the courts of the Republic of South Africa; and

16.3.2 Either Party may bring proceedings in any court of competent jurisdiction,

16.3.3 In respect of any action, claim or matter arising under or in connection with this DPA.

16.4 **Dispute resolution**. Any disputes arising from or in connection with this DPA will be brought exclusively before the competent court of the jurisdiction specified in clause 16.2 above.

16.5 **Counterparts**: This DPA may be executed in any number of counterparts, each of which will constitute an original, but which will together constitute one agreement. Where one or both of the parties chooses to execute this DPA by electronic signature, each electronic signature will have the same validity and legal effect as the use of a signature affixed by hand and is made to authenticate this DPA and evidence the intention of that party to be bound by this DPA.

17. MCi CONTACT POINT

17.1 Contact information of **MCi's** information officer:

Name: Aliki Droussiotis

Email: aliki@mci.co.za

18. PARTICULARS OF PROCESSING

18.1 **Categories of data subjects whose personal information is processed:**

18.1.1 **MCi** acknowledges that, depending on the Client's use of the Services, **MCi** may process the personal information of any of the following types of data subjects:

- The Client employees, contractors, temporary workers, agents and representatives
- The Client's Clients
- Applicant and/or candidate information
- Categories of personal information

18.1.2 **MCi** acknowledges that, depending on the Client's use of the Services, the types of personal information processed by **MCi** may include, but are not limited to the following:

- Basic personal information (for example first name, last name, email address and work address).
- Bank account information.
- Contact information (for example work email and phone number).
- Professional or employment-related information (for example, employer name and job title).
- Location information (for example, geo-location network data).

18.2 **Duration and object of processing:**

18.2.1 The duration of processing will be for the duration of the **Client Agreement** between the Client and **MCi**.

18.2.2 The objective of the data processing is the provision of Services.

18.2.3 Personal information may be processed on a continuous basis in order to provide the Services under the existing **Client Agreement**.

18.3 **Nature of the processing**

The personal information processed will be subject to the following basic processing activities:

18.3.1 Receiving information, including collection, accessing, retrieval, recording, and data entry.

18.3.2 Holding information, including storage, organisation and structuring.

18.3.3 Using information, including analysing, consultation, testing, automated decision making and profiling.

18.3.4 Updating information, including correcting, adaptation, alteration, alignment and combination.

18.3.5 Protecting information, including restricting, encrypting, and security testing.

18.3.6 Sharing information, including disclosure, dissemination, allowing access or otherwise making available.

18.3.7 Returning information to the Client or data subject.

18.3.8 Erasing information, including destruction and deletion.

18.4 **Purpose(s) of the processing and further processing**

The purpose of processing personal information is for **MCi** to provide the Services under the existing **Client Agreement.**

18.5 **The retention period**

See Clause 13 of the DPA.

18.6 **Data transfers to (sub-) processors**

In accordance with the DPA, **MCi** may engage sub-operators to provide Services on **MCi's** behalf. Any such sub-processors will be permitted to obtain personal information only to provide the Services **MCi** has engaged them to provide, and they are prohibited from using personal information for any other purpose.

19. TECHNICAL AND ORGANISATIONAL MEASURES

19.1 **Information Security Policy**

19.1.1 **MCi** shall develop, implement, maintain, and monitor a written information security policy that contains appropriate technical and organisational measures (ensuring a level of security appropriate to the risk presented by the Processing) to protect Personal Data against Security Breach and against all other unauthorised forms of Processing ("Information Security Policy").

19.1.2 **MCi** shall ensure that the Information Security Policy contains appropriate procedures to respond to a Security Breach.

19.1.3 MCi shall develop, implement and maintain a process for regularly testing, assessing, and evaluating the effectiveness of its Information Security Policy.

19.1.4 MCi shall update its Information Security Policy as required to effectively maintain the security of Personal Data.

19.1.5 MCi shall keep Personal Data logically separate to data Processed on behalf of any other third party.

19.1.6 MCi shall safeguard the security and confidentiality of all encryption keys associated with encrypted Personal Data.

19.1.7 MCi shall ensure that any person Processing Personal Data on the Operator's behalf will do so in compliance with this Clause 19.

19.2 **Organisational Security Measures**

19.2.1 MCi will maintain the following controls and safeguards applied to its employees:

- All employees undergo POPIA and Information Security awareness training annually.
- Employees can only access any dashboards and/or files containing Personal Data with Authentication and MFA (Multifactor Authentication) completed on access devices.
- All company provided access devices run centrally managed antivirus, firewall, threat control and anti-exploit software, which software is updated automatically.
- All company devices must be locked at all times when not in use with a 15-minute lockout window.
- Employees have access to document shredders and secure disposal bins.

19.3 **Physical Security Measures on Premises and Access Controls**

19.3.1 MCi will maintain the following access controls to the premises:

- Physical access controlled by locks and electronic tags.
- All employees are assigned unique access tags.
- All employee access is logged by entry point, date stamp and access tag identifier.
- Access control is limited to the employees' required level of access (i.e. the principle of least privilege is adhered to).
- Authorised access to systems by employees is reviewed on a regular basis.
- All doors to the premises are locked outside of working hours.
- Alarms at all entry locations.

19.4 **Network Security Controls**

19.4.1 MCi shall apply the following network security measures:

- Separate 'Guest' Wifi from "Company" WiFi network access, where the former is limited to pure internet breakout only and the latter includes access to company network resources.
- User access to WiFi networks is secured via a password.
- User access to the company LAN is secured via a domain authenticated profile (username and password).
- Firewalls are deployed to separate internal network zones and between these zones and public networks (i.e. the internet).
- Access to company shared files is secured via domain authenticated profiles and only accessible from company LAN or VPN.
- Remote user access to the company LAN is provided only via VPN secured via password and MFA.