DATA PRIVACY AND SECURITY

During the course of providing Services, Service Provider may obtain, access or otherwise Process Personal Data. Service Provider agrees to protect all Personal Data as detailed in this Annexure.

1) DEFINITIONS

a) "**Applicable Privacy Laws**" means all applicable privacy, information security, data protection, and data breach notification laws and regulations including but not limited to the POPIA.

b) "**Information Security Program**" means a comprehensive written information security program which complies with Applicable Privacy Laws, and contains appropriate administrative, technical, and physical safeguards to protect Personal Data against anticipated threats or hazards to its security, confidentiality or integrity (such as unauthorized access, collection, use, copying, modification, disposal or disclosure, unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage or any other unauthorized form of Processing).

c) "**Personal Data**" means any information in any form, format or media (including paper, electronic and other records), that identifies an individual or relates to an identifiable living individual and/or existing juristic person that (i) is provided by or on behalf of Company (or its employees, contractors or agents), (ii) Service Provider provided to or obtained for the Company or (iii) Service Provider Processes, in each case, in connection with the Services.

d) "**POPIA**" means the Protection of Personal Information Act No. 4 of 2013 and regulations, as amended from time to time.

e) "**Process**" or "**Processing**" or **"Processed"** means any operation or activity or any set of operations, whether or not by automatic means, concerning the collection, recording, organization, structuring, alteration, use, access, disclosure, copying, transfer, storage, deletion, combination, restriction, adaptation, retrieval, consultation, destruction, disposal or other use of Personal Data. The applicable Agreement describes the scope of the Service Provider's Processing.

f) "**Security Incident**" means any accidental or unauthorized access, acquisition, use, modification, disclosure, loss, destruction of or damage to Personal Data, or any other unauthorized Processing of Personal Data.

g) "**Sensitive Personal Data**" means any of the following types of Personal Data: (i) social security number, taxpayer identification number, passport number, driver's license number or other government-issued identification number; (ii) payment card (including credit or debit card) details or financial account number, with or without any code or password that would permit access to the account or credit history; or (iii) information on race, religion, ethnicity, sex life or practices or sexual orientation, medical or health information, genetic or biometric information, biometric templates, political or philosophical beliefs, political party or trade union membership, background check information or judicial data such as criminal records or information on other judicial or administrative proceedings.

2) DATA PROCESSING AND PROTECTION

a) **Compliance with Applicable Privacy Laws**. Service Provider will comply with Applicable Privacy Laws relating to Service Provider's performance under this Agreement and each applicable Statement of Works ("SOW"), where applicable.

b) **Limitations on Use.** Service Provider will Process Personal Data only on Colgate's behalf to deliver Services in accordance with this Agreement or Colgate's other documented instructions, whether in written or electronic form, such as an applicable SOW. The duration of the Processing will be the same as the duration of this Agreement or applicable SOW, if any, except as otherwise agreed to in this Agreement, the applicable SOW, or in writing by the Parties.

c) **Information Security Program.** Service Provider will implement, maintain, monitor and, where necessary, update its security features that will include the measures listed in the Security Standards attached hereto as Appendix 1.

d) **Data Integrity**. Service Provider will ensure that all Personal Data created or maintained by Service Provider on Colgate's behalf is accurate and, where appropriate, kept up to date, and will erase or rectify inaccurate or incomplete Personal Data in accordance with Colgate's instructions.

e) **Cross-Border Transfers**. Service Provider will ensure that Personal Data is not transferred to, accessed by or otherwise processed by its Service Provider Personnel in any country other than those specified in the applicable SOW, if specified, unless Colgate agrees in writing. If applicable, at Colgate's request, Service Provider (and if relevant, Service Provider's affiliates or subcontractors) will enter into an appropriate data processing agreement that incorporates the European Commission Standard Contractual Clauses between Controllers and Processors, or any similar agreement relating to other countries Applicable Laws, with Colgate to allow Colgate and Colgate's international offices to transfer Personal Data to Service Provider or such affiliates and/or subcontractors.

f) **Subcontracting**. Notwithstanding, and expressly in limitation of, anything to the contrary in the Agreement, Service Provider will not disclose or transfer Personal Data to, or allow access to Personal Data by, (each, a "**Disclosure**") any third party without Colgate's express prior written consent; provided, however, that Service Provider may Disclose Personal Data to its affiliates and subcontractors for purposes of providing the Services to Colgate, subject to the following conditions: (i) Service Provider will maintain a list of the affiliates and subcontractors to which it makes such Disclosures and will provide this list to Colgate upon Colgate's request; (ii) Service Provider will provide Colgate at least 30 days' prior notice of the addition of any affiliate or subcontractor to this list and the opportunity to object to such addition(s); and (iii) if Colgate makes such an objection on reasonable grounds and Service Provider is unable to modify the Services to prevent Disclosure of Personal Data to the additional affiliate or subcontractor, Colgate will have the right to terminate the relevant Processing. Service Provider will, prior to any Disclosure, ensure that such third party is bound by contractual obligations that are at least as restrictive as this Annexure. A copy of such contractual obligations will be provided to Colgate upon request. Service Provider will be liable for all actions by such third parties with respect to such Personal Data so Disclosed.

g) **Requests or Complaints from Individuals.** Service Provider will notify Colgate in writing, without undue delay (and in any event within 24 hours), unless specifically prohibited by laws applicable to Service Provider, if Service Provider receives: (i) any requests from an individual with respect to Personal Data Processed by or on behalf of Service Provider, such as opt-out requests, requests for access and/or rectification, erasure, restriction, requests for data portability, and all similar requests; or (ii) any complaint relating to the Processing of Personal Data, including allegations that the Processing infringes on an individual's rights. Service Provider (i) will not respond to any such request or complaint unless expressly authorized to do so by Colgate, (ii) will cooperate with Colgate with respect to any action taken relating to such request or complaint, whether received by Service Provider or Colgate, and (iii) will implement appropriate processes (including technical and organizational measures) to assist Colgate in responding to requests or complaints from individuals.

h) **Audit.** Service Provider will provide to Colgate, its authorized representatives, and such independent inspection body as Colgate may appoint, for the purpose of auditing Service Provider's compliance with its obligations under this Annexure, on reasonable notice: (i) access to Service Provider's information, processing premises, and records; (ii) reasonable assistance and cooperation of Service Provider Personnel; and (iii) reasonable facilities at Service Provider's premises.

i) **Regulatory Investigations.** Upon request by Colgate, Service Provider will assist and support Colgate in the event of an investigation by any regulator or authority, including a data protection authority, if and to the extent that such investigation relates to Personal Data Processed by Service Provider on Colgate's behalf in accordance with this Annexure.

j) **Security Incident**. Service Provider will notify Colgate in writing without undue delay (and in any event within 24 hours) whenever Service Provider reasonably believes a Security Incident has occurred. After providing notice, Service Provider will investigate the Security Incident, take all necessary steps to eliminate or contain the exposure of the Personal Data, and keep Colgate informed of the status of the Security Incident and all related matters. Service Provider further agrees to provide reasonable assistance and cooperation requested by

Colgate and/or Colgate's designated representatives, in the furtherance of any correction, remediation or investigation of any Security Incident and the mitigation of any potential damage, including any notification that Colgate may determine appropriate to send to affected individuals, regulators or third parties, and/or the provision of any credit reporting service that Colgate deems appropriate to provide to affected individuals. Service Provider will be responsible for all costs associated with such activities and will reimburse Colgate for the reasonable cost of notification to affected individuals, fielding feedback and questions from those notified, and any other reasonable associated costs that Colgate may incur in connection with responding to or managing the Security Incident, including, for example, costs relating to obtaining contact information for affected individuals, attorney's fees and legal costs, call center services and forensics services, credit monitoring, and other remediation costs. Unless required by law applicable to Service Provider, Service Provider will not notify any individual or any third party other than law enforcement of any potential Security Incident involving Personal Data in any manner that would identify, or is reasonably likely to identify or reveal the identity of, Colgate, without first obtaining written permission of Colgate.

k) **Return or Disposal of Personal Data.** Upon termination or expiration of its obligations under this Agreement or upon request of Colgate, whichever comes first, Service Provider shall (i) cease all Processing of and return to Colgate or, at the written request of Colgate, securely dispose of or securely destroy all Personal Data in the custody and control of the Service Provider (or agents or subcontractors, as applicable), in each case using appropriate physical, administrative and technical safeguards to protect such Personal Data against loss, theft and unauthorized access, disclosure, copying, use, or modification, and (ii) certify to Colgate, in writing, that Service Provider has complied with its obligations under this Section.

l) **Assistance**. Service Provider will provide appropriate information and assistance requested by Colgate to demonstrate Service Provider's compliance with its obligations under this Annexure and assist Colgate in meeting its obligations under Applicable Privacy Laws regarding: (i) registration and notification; (ii) ensuring the security of the Personal Data; and (iii) carrying out privacy and data protection impact assessments and related consultations with data protection authorities. In addition, when Service Provider is responding to Colgate's requests, Service Provider will inform Colgate if Service Provider believes that any Colgate instructions regarding the Processing of Personal Data would violate applicable law.

3) **AMENDMENT.** In the event that this Annexure, or any actions to be taken or contemplated to be taken in performance of this Annexure, do not or would not satisfy either party's obligations under Applicable Privacy Laws, the parties will negotiate in good faith to execute an appropriate amendment to this Annexure.

4) **INDEMNIFICATION**. Without limitation on any other indemnification obligations set forth in this Agreement, Service Provider hereby agrees to defend, indemnify and hold Colgate and its subsidiaries, and their respective employees, directors, officers, agents and equity holders, harmless from and against any and all Claims that arise out of a Security Incident. Further, Service Provider hereby agrees to defend, indemnify and hold Colgate and its subsidiaries, and their respective employees, directors, officers, agents and equity holders, harmless from and against any and all Claims that arise out of a breach of the representations and warranties contained in Section 6 of this Annexure.

5) **SURVIVAL.** The obligations of Service Provider under this Annexure will continue for so long as Service Provider continues to Process or possess Personal Data, even if all agreements between Service Provider and Colgate have expired or have been terminated.

6) **PERSONAL DATA PROVIDED BY SERVICE PROVIDER.** As part of the Services provided under this Agreement, Service Provider may provide Colgate with Personal Data. Service Provider represents and warrants that: (a) it has collected all such Personal Data in compliance with all applicable laws; (b) where required by law, it has provided notices to and received consents from individuals and that such notices or consents include the intended uses or disclosures of the Personal Data under this Agreement (including Processing by the Colgate for direct marketing to individuals); and (c) its sharing of Personal Data with Colgate and Colgate's use of Personal Data in accordance with the terms of this Agreement will not violate any Applicable Privacy Laws.

APPENDIX 1

SECURITY STANDARDS

At a minimum, Service Provider will take the security measures set forth in this Appendix.

1. **Physical Control Access / Physical Security**. Service Provider will take industry standard steps designed to prevent unauthorized persons from gaining access to Personal Data processing systems by maintaining industry standard physical security controls at all Service Provider sites at which an information system that uses or houses Personal Data is located.

2. **Logical/Data Access Control.** Service Provider will maintain appropriate access controls designed to prevent Personal Data processing systems from being used without proper authorization, including:

    a) restricting access to Personal Data to only authorized Service Provider Personnel who require such access in order to perform the Services and providing the lowest level of access required in accordance with the "least privilege" approach and to the minimum number; and

    b) implementing industry standard physical and electronic security measures to protect passwords or other access controls.

Further, Service Provider will:

    a) Maintain user administration procedures: define user roles and their privileges; define how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms; and

    b) Ensure that all employees of Service Provider and its subcontractors are assigned unique User-IDs.

3. **Data Transfer Control/Network Security**. Service Provider will ensure that: (a) Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control). Suppler will maintain network security using industry standard equipment and industry standard techniques, including firewalls, intrusion detection and prevention systems, and routing protocols; (b) it utilizes industry standard anti-virus and malware protection software to protect Personal Data from anticipated threats or hazards and protect against unauthorized access to or use; and (c) it utilizes industry-standard encryption tools (not less than 128-bit key utilizing an encryption method approved by Colgate) and other secure technologies in connection with any and all Personal Data that Service Provider: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; or (iii) stores on portable devices, where technically feasible (including safeguarding the security and confidentiality of all encryption keys associated with encrypted Sensitive Personal Data).

4. **Availability Control/Separation Control.** Service Provider will implement appropriate policies and procedures to ensure that: (a) it Processes Personal Data in accordance with Colgate's instructions; (b) it Processes separately Personal Data collected for different purposes; and (c) Personal Data is protected against accidental destruction or loss.

5. **Organizational Security.** Service Provider will maintain security policies and procedures to classify sensitive or confidential information, clarify security responsibilities and promote awareness for employees by, among other things: (a) maintaining adequate procedures regarding the use, archiving, or disposal of media containing Personal Data; and (b) managing Security Incidents in accordance with appropriate incident response procedures.

    c) Prior to providing access to Personal Data to Service Provider personnel, Service Provider will require Service Provider personnel to comply with its Information Security Program.

    d) Service Provider will maintain a security awareness program to train personnel about their security obligations. This program will include training about data classification obligations, physical security controls, security practices, and security incident reporting.

    e) Service Provider will maintain procedures such that (i) when media are to be disposed of or reused, any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory will be prevented; and (ii) when media are to leave the premises

at which the files are located as a result of maintenance operations, any undue retrieval of Personal Information stored on them will be prevented.

6. **Business Continuity**. Service Provider will maintain appropriate back-up, disaster recovery and business resumption plans, business continuity plan and risk assessment, and review and test these plans regularly to ensure that they are up to date and effective. Service Provider will maintain procedures for reconstructing lost Personal Data in Service Provider's possession or under Service Provider's control, and correct, at Colgate's request, any destruction, loss or alteration of any of Personal Data caused by Service Provider, or arising out of Service Provider's breach of this Agreement.

7. **Security Manager**. Service Provider will designate an employee ("Security Manager") who will be responsible for managing and coordinating the performance of Service Provider's obligations set forth in its Information Security Program and in this Annexure.

8. **Risk Assessments**. Service Provider will conduct periodic risk assessments and reviews and, as appropriate, update its Information Security Program; provided that Service Provider will not modify its Information Security Program in a manner that would weaken or compromise the confidentiality, availability or integrity of Personal Data.