ACCENTURE, INC.
Purchase Order Terms and Conditions

Definitions

"Agreement" means: (i) the applicable Purchase Order issued by Accenture; (ii) these General Terms and Conditions of Purchase; and (iii) additional written agreements, if any, relating to the transaction signed by Accenture and the indicated provider such as a master agreement, statement of work or letter agreement ("Additional Agreements").

The Agreement is the sole and exclusive agreement between the indicated Service Provider and Accenture with respect to the goods and/or services provided by the Service Provider under the applicable purchase order (collectively, **"Deliverables".)** By providing any Deliverables to Accenture, Service Provider agrees it is bound by the Agreement. Service Provider and/or Accenture may be referred to as a "Party" or "Parties" in these General Terms.

In the event of any conflict among the terms of Agreements, the following order of precedence will apply: (i) the Additional Agreements; (ii) the applicable Purchase Order issued by Accenture; and (iii) these General Terms.

"Accenture" means Accenture, Inc., a corporation registered and duly existing under the laws of the Philippines having its registered address at 7F Robinsons Cybergate Tower 1, Pioneer Street Mandaluyong City.

"Affiliate" means any entity, whether incorporated or not, that is controlled by or under common control with Accenture and its successors, where "control" means the ability, whether directly or indirectly, to direct the management and policies of another entity by means of ownership, contract or otherwise.

"Deliverables" means the goods and/or services, as the case may be, detailed in the Purchase Order.

"Intellectual Property Rights" means all intellectual and industrial property rights anywhere in the world including without limitation, any invention, patent, design or utility model rights, any copyright and trademarks, database rights, topography rights, commercial or confidential information, know how or trade secrets and any other rights of a like nature whether or not registered, and the right to apply for them.

"Purchase Order" means the attached Purchase Order form executed by Accenture requesting the supply of Deliverables.

"Service Provider" means the person or entity to which the Purchase Order is addressed. For avoidance of doubt, any reference to Supplier or Vendor herein shall also mean Service Provider in relation to this Agreement.

"Specification" means the specification; description; function; or any other requirements set out in the Purchase Order and attached documents (including drawings or descriptions) and the Service Provider's product documentation.

"Conditions" means these Terms and Conditions of Purchase.

1. Purchase Order

1.1 The Purchase Order issued by Accenture will set out the Deliverables required by Accenture. Service Provider agrees that any and all Deliverables stated in the Purchase Order shall be subject to these Conditions, except where Accenture and Service Provider have executed a separate agreement specifically applicable to the supply of such Deliverables, such agreement being endorsed by an authorized signatory of Accenture. In case a specific agreement is executed for a particular Purchase Order and/or Deliverables, the terms and conditions provided in that agreement which are inconsistent with these Conditions shall govern the supply of such Deliverables and shall prevail over these Conditions.

1.2 Subject to Clause 1.1, the parties agree that the Purchase Order together with these Conditions states all of the terms and conditions relating to the Deliverables specified in the Purchase Order, to the exclusion of any other terms and conditions relating to such Deliverables on any other purchase order, confirmation, invoice, payment slip or any other related document, and in particular, those documents issued by Service Provider.

1.3 In the event that the Service Provider has to design, develop or manufacture goods specified on the Purchase Order specifically for Accenture, the Service Provider shall first submit to Accenture a prototype and/or plan of such product for the approval of Accenture. The Service Provider must first obtain written confirmation from Accenture that the prototype and/or plans have been

accepted and full production of the goods can commence before commencing the work. Accenture will not be liable to reimburse the Service Provider for any costs incurred prior to receipt of this written confirmation from Accenture.

2. Delivery

2.1 With regard to performance of the Purchase Order by the Service Provider, time is of the essence. The Deliverables shall be delivered or performed on the date and at the place specified in the Purchase Order. Service Provider shall immediately inform Accenture of any foreseen or foreseeable delay in the delivery or performance of the Deliverables, and secure further instructions from Accenture regarding the delivery or performance of Deliverables.

2.2. Unless expressly agreed otherwise, the Deliverables shall be delivered during Accenture's normal business days. Delivery and any other costs associated with the supply of the Deliverables shall be at the Service Provider's own expense, unless otherwise stated in the Purchase Order.

2.3 Accenture's signature on any delivery receipt or other documentation presented for signature in connection with delivery of the Deliverables is evidence only of the number of packages and quantity received by Accenture and is not evidence of the actual quality or condition of the Deliverables. Notwithstanding this provision, Accenture shall inspect the Deliverables and perform Accenture's acceptance tests without undue delay following the delivery, taking into account the nature of the Deliverables.

2.4. In the event of delay in the delivery or performance of Deliverables by Service Provider not otherwise under the exceptional circumstances provided in this Agreement, or was not due to a fortuitous event or fault or negligence of Accenture, its employees, representative or agents , Accenture shall be entitled to received penalty in an amount equivalent to 1/10 of 1% of the price of the relevant deliverables as specified in the Purchase Order for each day (i.e. calendar day) of delay but not to exceed ten percent (10%) of the price of the deliverables which is/are delayed, until such performance has satisfactorily fulfilled. It is understood and agreed by both parties the herein penalty for delay shall be limited to delay in the delivery of the product/s only and shall not apply to other Service Provider's non-compliance with the other provisions of this Agreement. In additional, the Service Provider shall provide an acceptable written explanation to Accenture stating the reason/s for the delay

3. Specifications and Rejection

3.1 The Deliverables must in all respects conform with the Specifications. All Deliverables which are in the form of goods must be of sound materials, workmanship, and design (where Service Provider is responsible for the design of Deliverables), and the Deliverables must in all respects conform to relevant samples, patterns, prototypes and/or plans accepted by Accenture. All Deliverables which are in the form of services shall be performed in a sound manner and shall be free from all defects, including defects in installation and/ or design (to the extent that Supplier is responsible for the design).

3.2 All Deliverables must pass Accenture's acceptance tests. Accenture shall be entitled to reject all Deliverables that do not meet the provisions of Clause 3.1. If by the nature of the Deliverables any defects or any failure to conform with Clause 3.1 does not or would not become apparent (despite the carrying out of any examination) until after use, Accenture may reject the same even after a reasonable period of use.

3.3 Any Deliverables rejected under Clause 3.2 above must, at Accenture's request, be replaced or reperformed as the case may be by the Service Provider at the Service Provider's expense. Alternatively, Accenture shall have the option to cancel the Purchase Order in whole or in part pursuant to Clause 9 hereof. All rejected Deliverables will be returned to the Service Provider at the Service Provider's expense. Service Provider shall refund to Accenture all payments made for the rejected Deliverables.

3.4 In addition to the Specifications, Deliverables shall comply with the minimum warranties and conditions provided under Section 3, Chapter 4, Title VI (Sales), Civil Code, including the implied warranty of title, warranty against hidden defects or encumbrance, and warranty as to quality or fitness. If the Deliverables fail to comply with the above-mentioned warranties and conditions, the Service Provider shall, upon Accenture's request, replace or re-perform the Deliverables at the Supplier's sole expense. Alternatively, Accenture shall have the option to cancel the Purchase Order in whole or in part pursuant to Clause 9 hereof.

3.5. Notwithstanding Accenture's rights under Clauses 3.3, Accenture shall be entitled to return any goods to the Service Provider for a full refund within 15 days from date

of delivery without incurring any costs or charges whatsoever.

4. Inspection

4.1 The Service Provider shall permit Accenture access to its premises at any reasonable time in order to inspect the Deliverables in the course of manufacture, provision or storage. If, as a result of such inspection, Accenture determines that the Deliverables does not meet the Specifications and/or will not comply with the Purchase Order, Accenture shall notify the Service Provider in writing and the Service Provider shall, as soon as possible, take all necessary steps to ensure compliance. The conduct of inspection or the delivery of notification by Accenture under this Clause shall not relieve the Service Provider of its obligations under the Purchase Order.

5. Ownership and Risk

5.1 Ownership and risk over Deliverables shall be transferred from Service Provider to Accenture upon delivery thereof pursuant to Clause 2 of this Terms and Conditions. Such passing of ownership and risk shall be without prejudice to any right of rejection of Deliverables under Clause 3 of this Terms and Conditions.

6. Prices and Payment

6.1 Prices and the currency shall be as specified in the Purchase Order (PO). For the avoidance of doubt, prices quoted in the Purchase Order are exclusive of the Value-Added Tax (VAT), which shall be applied in addition to the prices when applicable. In view of the registration of Accenture with the Philippine Economic Zone Authority (PEZA), sales of goods and services to the PEZA sites of Accenture shall be subject to 0% VAT. In the case of Deliverables which are for the account of Accenture's non-PEZA sites, any VAT due on the purchase shall be billed as a separate item. For the avoidance of doubt, the term "non-PEZA site" of Accenture shall include sites for which the application for PEZA registration has been filed and still pending with the PEZA. Refer to the comment section of the PO for explicit instruction if transaction is vatable.

Payments to be made by Accenture under the PO shall be subject to withholding taxes, when applicable. The Certificate of Withholding Tax shall be provided by Accenture to the Service Provider not later than twenty (20) days from the close of the quarter when the payment was made in compliance with existing tax laws and regulations.

6.2 The prices and quantity quoted in the Purchase Order shall not be increased by Service Provider, unless agreed upon in writing by Accenture. Proposed changes on price and quantity must be communicated to the requestor to initiate PO Change Order. Invoicing is discouraged without the amended PO.

6.3 Service Provider shall ensure that all invoices submitted to Accenture are current (i.e. invoices should be received by Accenture within Five (5) days from the time services were rendered or goods were delivered) and are valid and correct. To be considered valid and correct invoice must comply with invoicing requirements for Accenture Philippines as captured on this link: https://www.accenture.com/us-en/about/company-suppliers-guide. In the event that Accenture is not able to receive invoices within five (5) days from time services were rendered or goods were delivered, any and all invoices must still be billed by Service Provider and received by Accenture within Ninety (90) days from delivery date, service period end date or applicable billing cycle. In case of any dispute/issue resulting in the non-processing of invoice, Service Provider shall complete necessary actions needed to process said invoices such as, but not limited to, the resubmission of corrected invoice for rejected invoice within Ninety (90) days from delivery date, service period end date or applicable billing cycle. Service Provider hereby waives its right to receive payment on any invoice received by Accenture more than Ninety (90) days from delivery date or service period end date or applicable billing cycle. Accenture shall neither honor nor process any invoice received after Ninety (90) days from delivery date, service period end date or applicable billing cycle.

6.4 After receipt of the invoice, or the corrected invoice as the case may be, within the Ninety (90) day period mentioned above Accenture shall pay the Service Provider in accordance with the payment terms specified in the Purchase Order, except for final billings that are subject to credit adjustments as provided in 6.10.

6.5 Service Provider shall ensure that all the information stated in the invoices are complete and accurate, matches with the PO, and that the specific requestor and financial charge codes or job numbers provided by Accenture are indicated therein. Invoices not supported by a Purchase Order with sufficient balance shall be rejected. Accenture shall strictly enforce "**No PO No Payment**" policy.

6.6 Accenture agrees to pay the Price to the Service Provider on satisfactory and compliant invoices based on

the agreed payment term commencing from the date of acceptance of invoice.

6.7 The Service Provider shall submit invoice to Accenture within (5) days after date of service or delivery of goods to RTP Drop Box area only as mentioned in Annex C – Invoice Receiving Channel, which is made an integral part of this Agreement. Invoices routed to other channels or contacts will not be honored.

6.8 Accenture shall accept submitted invoice that conforms to *BIR Revenue Regulation 18-2012 and Section 6.B Information Contained in the Invoice of Revenue Regulation 7-2024. In addition, converted Official Receipts/Billing Statement/Statement of Account/Billing charges must adhere to provisions under Revenue Regulation 11-2024 and Revenue Memorandum Circular 77-2024.*

6.9 Payments shall be settled by way of electronic fund transfer and any inward bank charges shall be borne by the Service Provider.

6.10. Accenture and its affiliates shall withhold payment of the final billing for the last services or deliverables identified under this Agreement. Both parties through its POCs shall coordinate with each other within sixty days from the completion of the last service or deliverable to finalize any credit adjustments. The withheld amount equivalent to the final billing shall be offset to any Credit Memo amounts owed by Service Provider to Accenture. If the invoices of the Service Provider are not sufficient to cover the Credit Memos, the former shall immediately refund Accenture, Inc. the remaining balance upon written notice of the latter.

If no Credit Memos are outstanding upon confirmation of the POCs or if there are still amount due to Service Provider after offsetting the final bill to the Credit Memo, Accenture shall pay such amount to Service Provider within the term indicated in the Agreement from the parties' confirmation in writing on the accuracy and completeness of the final credit adjustments or of no outstanding Credit Memo, provided, that the parties shall not unreasonably withhold such confirmation

6.11. During the term of this Agreement and for a period of three (3) years thereafter, Supplier will retain and, upon reasonable notice, will provide Accenture reasonable access to audit Supplier's books, accounts, and records relating to the Deliverables. At the Supplier's option, Accenture may select an independent third party of international reputation and good standing to conduct the audit. Any such independent third party will be required to an appropriate confidentiality/non-disclosure agreement. Supplier shall cooperate fully in any audit conducted by or on behalf of Accenture.

7. Intellectual Property Rights

7.1 Service Provider warrants that the sale or use of goods, or the performance or provision of the Deliverables will not violate or infringe any Philippines or foreign copyright, patent, trademark, registered design or any other Intellectual Property Rights. Service Provider warrants that all Intellectual Property Rights on the pre-existing materials used by Service Provider in the provision of Deliverables to Accenture are owned by the Service Provider. Notwithstanding the above, the Service Provider hereby grants Accenture an irrevocable license to use, copy or modify such pre- existing materials for internal business purposes, free of royalty payments or any other charges.

7.2 The Intellectual Property Rights in all works of authorship developed or created by Service Provider in the course of provision of Deliverables ("Project Materials") shall immediately and exclusively vest in Accenture. In the event that the Service Provider requests and Accenture grants written consent that the Intellectual Property Rights for specific Project Materials be not assigned to Accenture, Service Provider shall grant to Accenture and its affiliates an irrevocable royalty-free license to use, copy or modify the Project Materials, with right to sub-license such Project Materials to third parties for the purposes intended by Accenture upon notice to Service Provider.

7.3 To the extent permissible under the applicable law, the Service Provider hereby waives all moral rights (as defined under the Law on Copyright, RA No. 8293) in the Project Materials supplied hereunder in so far as they relate to Accenture and agrees that it has obtained all waivers of moral rights and consents from any employee, agent, subcontractor or other third party necessary to comply with its obligations under this Clause 7.

7.4 Any drawings, specifications, data, documents, and other information provided by Accenture to the Service Provider in connection with the Purchase Order and all Intellectual Property Rights therein shall remain the property of Accenture, and the Supplier shall at all times keep confidential all such information. Service Provider shall take adequate procedures to protect the secrecy of such drawings, specifications, data, documents, and other information, and shall return the same to Accenture upon completion of the Purchase Order.

8. Liability

8.1 Service Provider shall indemnify Accenture against any losses, costs and/or liabilities that may be incurred by Accenture as a result of any action, claim or demand that a third party might make by reason of any breach by the Service Provider of these Conditions, the warranties and conditions provided under Section 3, Chapter 4, Title VI (Sales), Civil Code, or any other statute relevant to supply of Deliverables.

8.2 Unless expressly agreed otherwise in writing, the Service Provider grants a full warranty for the Deliverables for a period of two (2) years commencing on the date when ownership and risk over the Deliverables are transferred to Accenture pursuant to Clause 5 of this agreement.

8.3 Any defective Deliverables must, at Accenture's option, be repaired, replaced or re-performed as the case may be by the Service Provider at the Service Provider's sole expense. Alternatively, Accenture shall have the option to cancel the relevant Purchase Order in whole or in part pursuant to Clause 9 of this agreement. All defective Deliverables will be returned to the Service Provider at the Service Provider's expense. Service Provider shall refund to Accenture all payments made for the defective Deliverables.

9. Indemnification

Service Provider will indemnify and hold harmless Accenture and its affiliates, and their partners, agents, and employees from all liability or expense (including but not limited to reasonable attorneys' fees and costs of investigation and defense) resulting from either (a) bodily injury to any person (including injury resulting in death) or damage to property arising out of the performance of this Agreement, provided such injury or property damage is due or claimed to be due to the acts, negligence or willful misconduct of Service Provider, its employees, agents, or subcontractors; (b) any claim that any Deliverable delivered under this Agreement, or use thereof by Accenture, infringes any patent, copyright, trademark, trade secret or other proprietary right of any third party; (c) negligence, recklessness or willful misconduct of the Service Provider or Service Provider employees in the provision of the Deliverables; (d) a breach by Service Provider or Service Provider Employees of any of the terms herein; (e) any claim, that the Service Provider 's Deliverables, related actions or omissions of the Service Provider , or the Service Provider employees, agents, or sub-contractors in any way connected therewith have violated any law or regulation; (f) any demand or claims for fees including damages from Service Providers' employees, agents and its employees; (g) any unauthorized act or omission by the Service Provider or Service Provider employees; (h) any finding, by any competent authority, of an employment relationship between Accenture and any Service Provider employee; or (i) any violations of Data Privacy laws, rules, or regulations. The indemnities provided under this Agreement shall be in addition to and not in lieu of any other remedy available to Accenture under this Agreement or by law.

10. Cancellation

Accenture reserves the right to cancel in whole or in part a Purchase Order, or any consignment on account thereof, pursuant to Clauses 2.4 (delay), 3.1, 3.2, 3.3 (defects or failure to comply with Specifications), 3.4 (implied warranties), 3.5 (returned goods), 8.3 (defective Deliverables), and (delay not withstanding implementation of BCP) of this agreement. If Accenture cancels the Purchase Order in whole or in part, Accenture shall only be obliged to pay for the Deliverables which were expressly accepted by Accenture. In the event that Accenture is constrained to purchase Deliverables of similar description and quality from a third party, by reason of the cancellation of the Purchase Order, Accenture shall be entitled to claim from Service Provider the incremental amount paid to the third party vendor for the purchase of Deliverables.

11. Anti- Corruption and Compliance with Laws

11.1 **Compliance with Laws.** Service Provider warrants that it is in compliance with all applicable federal, state and local laws, regulations and standards, including but not limited to, those relating to the design, manufacture, testing, labeling, sale and transportation of the Products, and provision of the Deliverables. Service Provider warrants that it is legally authorized to engage in business in the Philippines and will provide Accenture satisfactory evidence of such authority upon request. Service Provider and its employees covenant to comply at all times with all applicable laws and regulations including the U.S. Foreign Corrupt Practices Act ("FCPA"), the UK Bribery Act and all other applicable anti-corruption laws, anti-competition laws, and export compliance laws. Further, if applicable, Service Provider and its subcontractors shall comply with the U.S. 28 C.F.R. Part 202, the DOJ Final Rule Implementing Executive Order 14117 (The DOJ Bulk Data Rule"). Service Provider will not take any action, or fail to take any action, that would result in Accenture violating any such law, rule, ordinance or regulation.

11.2 In the event of a breach of the anticorruption

provisions set forth in this Agreement, Accenture shall, in its sole discretion and in addition to any other remedies it may have under the law or this Agreement, terminate this Agreement immediately.

11.3 **Tax Evasion.** Each Party has established, maintains and enforces policies, processes and controls as required by law and in accordance with any regulation or published guidance of tax authority to prevent the facilitation of tax evasion. The Parties agree to notify each other in writing within a reasonable timeframe of a breach of this Section or an attempt to facilitate tax evasion (either by the relevant Party or any other third-party) where this may affect the provision or receipt of the Provider Offerings or the operation of the Parties' businesses or the Parties' compliance with tax evasion law. A breach of the Section is deemed a material breach in accordance with the relevant "Termination" Section.

11.4 **Compliance with Environmental Laws, Regulations, and Standards**. Accenture is committed to incorporating leading environmental practices into its business strategy and operations and to fostering environmental awareness and responsibility among our stakeholders, including employees, clients and service providers/suppliers.

Service Provider undertakes to comply with all applicable environmental laws, regulations and standards. Service Provider further commits to reduce their negative environmental impact and provide visibility to their progress toward this commitment, and to encourage the development and use of environmentally friendly technologies and practices and the reduction of negative environmental impacts through their supply chain. Failure to comply with these standards or with applicable laws and regulations may result in termination of this Agreement as well as Service Provider's accreditation as an Accenture vendor, and referral of the matter to local authorities.

11.5 **Compliance with Occupational Safety and Health (OSH) Laws, Regulations, And Standards**. Accenture is committed to incorporating leading OSH practices into its business strategy and operations and to fostering occupational safety and health awareness and responsibility among our stakeholders, including employees, clients and service providers/suppliers.

Service Provider undertakes to comply with all applicable occupational safety and health laws, regulations and standards. Failure to comply with these standards or with applicable laws and regulations may result in termination of this Agreement as well as Service Provider's accreditation as an Accenture supplier, and referral of the matter to local authorities.

12. Code of Business Ethics

12.1 Provider must comply with the Accenture Supplier Standards of Conduct [Supplier Standards of Conduct | Accenture], as updated by Accenture from time to time (the 'Accenture Supplier Standards'). Without prejudice to the foregoing, Provider:

a. warrants and represents to Accenture that it: (1) conducts risk-based human rights and environmental due diligence in its supply chain as appropriate; and (2) requires its own direct suppliers to comply with equivalent obligations to those set out in the Accenture Standards; and

b. must report to the Accenture Business Ethics Helpline any suspected or actual violations of the Accenture Standards.

12.2 Accenture has established reporting mechanisms and prohibits retaliation or other adverse action for reporting violations of these standards. To report a serious concern, please call the Accenture Business Ethics Line at +1 312 737 8262, available 24 hours a day, seven days a week (you can reverse the charges) or visit the encrypted website at https://businessethicsline.com/accenture. You should use the Ethics Line only to make a good faith claim. Accenture takes all allegations seriously.

12.3 No Conflicts. Service Provider affirms that to the best of its knowledge neither it nor its officers, partners, employees, permitted subcontractors and/or agents have knowledge of any existing or potential interest in conflict with the Deliverables under a Purchase Order or this Agreement that could reasonably be considered to: (a) negatively impact its participation during execution of Deliverables; (b) cause it or Accenture to violate any law or regulation; or (c) create any appearance of impropriety (each a "Conflict"). If either party becomes aware of a Conflict during the term of this Agreement, it will promptly bring the matter to the attention of the other party and the parties will work together to reach a mutually satisfactory resolution; if such mutually satisfactory resolution cannot be reached within a reasonable period of time (not to exceed ten (10) business days after first notice, unless mutually agreed), then Accenture may immediately terminate this Agreement or the affected part of a Purchase Order.

13. General

13.1 The Service Provider agrees: (a) that it shall comply

with all applicable data protection and privacy laws, and regulations, including but not limited to Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation ("GDPR") and the Philippine's Data Privacy Act of 2012 ("DPA") (together, the "Data Protection Laws") and the Data Privacy Schedule hereto attached as **ANNEX A** and made an integral part hereof, in relation to the Purchase Order and other information received from Accenture; and (b) that it shall not, by any act or omission, put Accenture in breach of any of the Data Protection Laws, in connection with the Purchase Order.

13.2 **Confidential Information**

13.2.1 **Definition.** Confidential Information shall refer to any information belonging to Accenture which:

a.) During the course of the performance of the Deliverables or Services, each party may be given access to (in any form) that relates to the other's past, present, and future research, development, business activities, products, services, and technical knowledge; OR
b.) Is identified by the discloser as confidential; OR
c.) Refers to any and all information relating to, belonging, referring to or in any manner pertaining to Accenture's clients; OR
d.) By its very nature is or would be understood to be confidential by a reasonable person under the circumstances (hereafter "Confidential Information).

13.2.2 **Use**. Service Provider may use or make copies of the Confidential Information of Accenture only to the extent reasonably necessary for purposes of this Agreement.

13.2.3 **Protection.** Service Provider will protect the confidentiality of the Confidential Information of Accenture in the same manner that it protects the confidentiality of its own similar confidential information, but in no event using less than a reasonable standard of care. Service Provider will restrict access to the Confidential Information to those of its personnel (including such personnel employed by its affiliates) and subcontractors engaged in the performance, management, receipt or use of the Deliverables or Services under this Agreement, provided that such parties are bound by obligations of confidentiality substantially similar to the terms of this Agreement.

13.2.4 **Return.** Service Provider will return or destroy Accenture's Confidential Information in its possession upon request by Accenture, unless otherwise allowed to retain such Confidential Information. Subject to applicable laws and notice to Accenture, Service Provider may retain copies of the other party's Confidential Information required for compliance with its recordkeeping or quality assurance requirements (subject to the terms of this Agreement).

13.2.5 **Exceptions.** Nothing in this Agreement will prohibit or limit a party's use of information (including, but not limited to, ideas, concepts, know-how, techniques, and methodologies) (a) previously known to it without an obligation not to disclose such information, (b) independently developed by or for it without use of the information, (c) acquired by it from a third party which is not, to the receiver's knowledge, under an obligation not to disclose such information, or (d) which is or becomes publicly available through no breach of this Agreement.

13.2.6 **Compelled Disclosure.** If the receiver receives a subpoena or other validly issued administrative or judicial process requesting Confidential Information of the other party, it will promptly notify the other party of such receipt and tender to the other party the defense of such subpoena or process. If requested by the other party, the receiver will reasonably cooperate (at the expense of the other party) in opposing such subpoena or process. Unless the subpoena or process is timely limited, quashed or extended, the receiver will then be entitled to comply with such request to the extent permitted by law.

13.3 The Service Provider shall have in force and maintain at the Service Provider's cost such policies of insurance with a reputable and authorized insurer that give adequate levels of insurance cover in respect of all of the Service Provider liabilities and obligations to Accenture in relation to the Purchase Order, at an amount acceptable to Accenture, and shall, upon request by Accenture, provide evidence of such policies. If Service Provider shall have any access to personal data under the Agreement, such insurance will include cyber liability (data privacy) coverage.

13.4 The Purchase Order shall not be assigned, charged, transferred or otherwise encumbered in whole or in part by the Service Provider without the prior written consent of Accenture.

13.5 Service Provider will not assign, transfer or subcontract the Agreement or Deliverables or its rights or obligations (including its data privacy obligations) to any third party (whether resulting from a change of control, merger or otherwise) to any third party (whether resulting from a change of control, merger or otherwise) without Accenture's prior written consent. The appointment of a subcontractor shall not relieve Service Provider of its

obligations (including data privacy obligations) under this Agreement. In any event, Service Provider will remain solely responsible for any and all acts, errors or omissions of its subcontractors (including its sub-processors).

13.6 The waiver by either party of a breach or default in any of the provisions of this agreement by the other party shall not be construed as a waiver of any succeeding breach of the same or other provisions; nor shall any delay or omission on the part of either party to exercise or avail itself of any right, power or privilege that it has or may have hereunder operate as a waiver of any breach or default by the other party.

13.7 If any part of these Conditions is found by a court of competent jurisdiction or other competent authority to be invalid, unlawful or unenforceable then such part will be severed from the remainder of these Conditions which will continue to be valid and enforceable to the fullest extent permitted by law.

13.8 Subject to Clause 1.1, the Purchase Order contains the entire agreement between the parties and supersedes all negotiations, representations (except fraudulent representations) and proposals (written and oral) relating to its subject matter.

13.9 These Conditions or any document or agreement made pursuant thereto may not be amended, modified or waived in any respect whatsoever, except in writing signed by the parties.

13.10 Any person who is not a party to this agreement shall have no rights under this agreement.

13.11 The parties hereby agree that the provisions of Clauses 7, 8, 9 and 11.1 hereof shall survive the termination of this agreement.

13.12 The Service Provider acknowledges that it is engaged as an independent contractor, and nothing in these Conditions or any Purchase Order shall be deemed or construed to create a joint venture, partnership, or employee/employer relationship between Supplier and Accenture.

13.13 These Conditions and any Purchase Order shall not be an exclusive agreement between the parties. Nothing shall prevent Accenture from procuring services or goods which are the same as or similar to the Deliverables from any third party.

13.14 Each party agrees that it has not been induced to agree to these Conditions by any representation other than that expressly set out herein or in any Purchase Order.

13.15 All aspects relating to the Conditions shall be subject to and interpreted in accordance with Philippine Laws. The parties submit to the exclusive jurisdiction of the local courts.

13.16 Accenture's rights, benefits and/or obligations under this Agreement may be assigned or transferred to any Affiliate. Service Provider hereby provides its consent in advance for such assignment or transfer.

13.17 **Information Security.** When the circumstances warrant and whenever applicable, the parties fully understand and agree to abide by Information Security Guidelines of Accenture and Work from Home Guidelines, which is hereto annexed as "**ANNEX B**" and made an integral part of this Agreement.

13.18 **Dispute Resolution.** The parties will make good faith efforts to first resolve internally any dispute under this Agreement by escalating it to higher levels of management. Any dispute, controversy, or claim arising out of, relating to, involving, or having any connection with this Agreement or otherwise related to the Project, including any question regarding the validity, interpretation, scope, performance, or enforceability of this dispute resolution provision, will be exclusively and finally settled by arbitration in accordance with the arbitration laws of the Philippines. The arbitration will be conducted in Mandaluyong City, unless the parties agree on another location by three arbitrators, with each party selecting one arbitrator and the third selected by both parties. The parties will be entitled to engage in reasonable discovery, including requests for production of relevant non-privileged documents. Depositions and interrogatories may be ordered by the arbitral panel upon a showing of need. All decisions, rulings, and awards of the arbitral panel will be made pursuant to majority vote of the three arbitrators. The award will be in accordance with the applicable law, will be in writing, and will state the reasons upon which it is based. The arbitrators will have no power to modify or abridge the terms of this Agreement.

13.19 **Business Continuity Plan.** Service Provider warrants that it has in effect a Business Continuity Plan ("BCP") as described in its response to the request for proposal in connection with this Agreement, if any, and that Service Provider shall maintain such BCP in effect for the term of this Agreement or Purchase Order. Such BCP plan should include, among others, Work from Home arrangements when applicable, in which case Service Provider shall ensure its compliance with pertinent Information Security

Protocols and Work from Home Guidelines under this Agreement or as may further advised by Accenture. Service Provider shall test its BCP a minimum of once each calendar year and inform Accenture in writing within 30 days of conducting such tests that such testing has been completed and (a) list any deficiencies revealed, or (b) confirm that no deficiencies were found. Service Provider shall allow Accenture to audit its BCP and test results at least once in a year or in the event of a material change to the BCP. Service Provider shall notify Accenture with at least sixty (60) days prior written notice of any intention to substantially modify or terminate such BCP. In the event that Service Provider (a) does not have a BCP in effect on the Effective Date of this Agreement, (b) did not respond to a request for proposal or (c) did not include a BCP in its response to a request for proposal in connection with this Agreement, Service Provider shall establish a detailed BCP and provide it to Accenture no later than thirty (30) days following the Effective Date of this Agreement and such BCP shall be subject to Accenture's written approval. Upon approval, such BCP shall be considered the BCP referred to in this section and shall be subject to the foregoing terms.

13.20 **Root Cause Analysis.** Promptly after receipt of a notice from Accenture of Service Provider's failure to meet the Deliverable or each time there occurs a failure to provide any Deliverables due to system outages or interruptions, Service Provider shall (i) commence diligent efforts to perform a root cause analysis, (ii) within five (5) days, unless Accenture requires a shorter period to comply with contractual requirements, provide a preliminary root-cause analysis for such failure, (iii) within ten (10) days, unless Accenture requires a shorter period to comply with contractual requirements, provide a final root-cause analysis for such failure, (iv) correct such failure within a reasonable time period not exceeding thirty (30) days, unless Accenture requires a shorter period to comply with contractual requirements, taking into account the circumstances, (v) provide Accenture with a report detailing the cause of and procedure for correcting such failure, (vi) provide Accenture with procedure for preventing the recurrence of the failure and (vii) provide Accenture reasonable evidence that such failure will not be repeated. Service Provider shall prioritize any root cause analysis performed hereunder at a level equal to or higher than that afforded to its testing or quality assurance investigations or activities conducted internally or for any other of such its customers or services reasonably comparable to the Services. All costs relating to correcting the problem based on the results of the root cause analysis shall be borne by the Service Provider. All Service Levels shall remain in effect notwithstanding the subsequent correction of any performance problem.

13.21 **Publicity.** Absent Accenture's prior written consent that may be withheld at Accenture's discretion, Service Provider may not communicate or publicize the existence of any business relationship established by this Agreement except internally. Absent Accenture's prior written consent which may be withheld at Accenture's discretion, Service Provider will not use Accenture's or Accenture's Affiliates' names or trademarks in connection with any advertising or promotional materials or activities, in a Web site, in a press release, or in other written, electronic, magnetic or laser media communications with, or services, materials or products provided to, third parties.

14. Effectivity

14.1 The Purchase Orders issued by Accenture do not require manual signatures and are presumed to have undergone the necessary approval process. The Purchase Order constitutes a valid offer on the part of Accenture and shall constitute a binding agreement between the Service Provider and Accenture upon acceptance by Service Provider.

14.2 The Purchase Order and these Terms and Conditions shall become valid and binding between Accenture and Service Provider upon Accenture's receipt of confirmation and acceptance from the Service Provider.

Unless otherwise agreed by the parties, Service Provider is obligated to accept the Purchase Order and these Terms and Conditions within three (3) business days after transmittal of the Purchase Order. The Service Provider's acceptance of the Purchase Order constitutes confirmation of the availability of Deliverables, and the Service Provider's undertaking to deliver the Deliverables within the period(s) stated in the Purchase Order.

15. Termination

15.1 Accenture may terminate the Agreement for its convenience (for any or no reason) at any time, in whole or in part, by providing thirty (30) days prior written notification to Service Provider. In the event of such termination, Service Provider will be entitled to payment of all fees and reimbursement of expenses, as provided in the relevant Purchase Order, incurred prior to the effective date of such termination. Unless expressly provided for in the Agreement or Purchase Order, Accenture will have no obligation to pay any early termination fee or extra charges in relation to such

termination.

15.2 **Transition Assistance.** When the circumstances warrant based on the nature of the Deliverables provided, upon termination of the Agreement for any reason, Service Provider shall extend transition assistance to Accenture for a reasonable, mutually agreed period of time after the expiration or termination of this Agreement. In principle, both parties agree that the transition assistance will allow for the expired or terminated portion of the Deliverables to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Deliverables to Accenture or to another party identified by Accenture to replace Service Provider. Such orderly transfer and transition assistance may include, but is not limited to, both parties meeting in good faith and in a timely manner to establish a Transition Management Plan laying down the respective roles and responsibilities of each party. The parties hereby agree that such transition assistance is governed by the terms and conditions of this Agreement, except for those terms or conditions that do not reasonably apply to such transition assistance.

15.3 **Public Health Emergency**

15.3.1 In the event that the Deliverable /s within the scope of this Agreement will be performed or proceed during a public health emergency (such as COVID19 Pandemic and/or other similar or related virus or health circumstances), Service Provider warrants that it will acquaint itself and strictly comply with the applicable laws, rules and regulations, risks, reasonable requirements, protections, and potential effects of such public health emergency including, without limitation, to possible effects on this Agreement, the Project, services provided and/or any and all persons performing or otherwise participating in any part of the foregoing. Service Provider further warrants that it will continue to perform the Deliverables for no more than the agreed upon fees and within same service level expectations and Contract Period. Further, Service Provider agrees to reasonably cooperate with Accenture in order to comply with requirements aimed at ensuring continuity of its Deliverables to Accenture.

15.3.2 Accenture and Service Provider hereby agree that if after the Effective Date, a governmental or quasi-governmental authority issues any order, regulation, requirement or other rule that requires Service Provider to cease performance of its Deliverables as a result of the aforementioned public health emergency and/or any other related cause, the Parties will promptly confer in good faith to determine whether each agrees, in its respective determination, to an equitable change in service level expectations or Contract Period. Service Provider shall support all such requests for additional or modified Contract Period with adequate supporting documentation. Any agreed change to such time/period must be in writing and signed by both Parties. Service Provider shall at all times use commercially reasonable best efforts to minimize any impact by any public health emergency/events related thereto on the Project, this Agreement and the Deliverables provided to Accenture.

ANNEX A

DATA PRIVACY SCHEDULE

This data privacy schedule ("Data Privacy Schedule") is subject to the terms and conditions of the Agreement. Terms not defined herein shall have the meaning set forth in the Agreement. In the event of a conflict between the Agreement and this Data Privacy Schedule, this Data Privacy Schedule shall prevail. Provider's failure to comply with any of the provisions of this Data Privacy Schedule shall be deemed a material breach of the Agreement.

1. DEFINITIONS

"Accenture Personal Data" means Personal Data owned, licensed, or otherwise controlled or Processed by Accenture or by Accenture's Affiliates (including Personal Data Processed by Accenture or by Accenture's Affiliates on behalf of Accenture's clients).
"Data Privacy Laws" means all applicable laws, regulations and regulatory guidance in relation to the Processing or protection of Personal Data, as amended from time-to-time.
"EEA Personal Data" means Accenture Personal Data which originates from a member state of the European Economic Area.
"Information Security Obligations" means commercially reasonable and appropriate physical, technical and organisational security measures, including those set forth in the Agreement and its Schedules.
"Personal Data" means any information relating to, identifying, describing, or capable of being associated with or reasonably linked (directly or indirectly) to, a natural person or household, and any other information regulated by Data Privacy Laws.
"Process" means any operation, or set of operations, which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. "Processes" and "Processing" shall be construed accordingly. Processing includes sub-Processing.
"Security Incident" means a known, or reasonably suspected, accidental or unauthorized loss, acquisition, disclosure, access, use or other form of compromise of Accenture Personal Data.
"Sub-processor" means any entity which Processes Accenture Personal Data on behalf of Provider.

2. SCOPE AND APPLICATION

This Data Privacy Schedule governs Provider's access to, and Processing of, Accenture Personal Data, where Provider accesses and/or Processes Accenture Personal Data on behalf of Accenture.

3. GENERAL PROVISIONS

3.1. **Compliance with Data Privacy Laws.** Provider shall comply with Data Privacy Laws in relation to its Processing of Accenture Personal Data.

3.2 **Compliance with Security Incident Laws.** Provider shall implement and maintain Information Security Obligations to protect Accenture Personal Data against a Security Incident. Provider shall fully assist and cooperate with Accenture and its clients in their compliance with applicable security incident laws. In particular, Provider shall: (i) notify Accenture in writing without undue delay, and in any event within forty-eight (48) hours, whenever a Security Incident has occurred; and (ii) investigate the Security Incident, taking all necessary steps to eliminate or contain the exposure, including cooperating with Accenture's investigation and remediation efforts, mitigating any damage, and developing and executing a plan, subject to Accenture´s approval, that promptly reduces the likelihood of a recurrence of the Security Incident.

3.3 **Retention and Deletion of Accenture Personal Data.** Provider shall not retain any Accenture Personal Data for longer than is necessary for the performance of the services and/or the fulfilment of its obligations under the Agreement, or as required or permitted by applicable law. Upon expiration or termination of the provision of services relating to the Processing of Accenture Personal Data, or at any time upon Accenture's request, Provider shall promptly and securely delete (or return to Accenture) all Accenture Personal Data (including existing copies), unless otherwise required by applicable laws.

3.4 **No Provider Access to EEA Personal Data.** The parties acknowledge that EEA Personal Data is not within the scope of the Agreement, including this Data Privacy Schedule. In the event that Provider will access or Process EEA Personal Data, Provider shall:

3.4.1 ensure that such access and Processing of EEA Personal Data complies with Data Privacy Laws; and

3.4.2 ensure that the international transfer of Personal Data (including any EEA Personal Data) complies with Data Privacy Laws, enter into any additional agreement(s) and/or legally valid data transfer mechanism(s) reasonably requested by

Accenture, governing the access, Processing and international transfer of Personal Data, and , when acting as data importer) explicitly acknowledge that: (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data; (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require Provider to create or maintain back doors or to facilitate access to personal data or systems or for Provider to be in possession or to hand over the encryption key.

4. PROCESSING ACCENTURE PERSONAL DATA

4.1 If Provider Processes Accenture Personal Data, Provider shall:

4.1.1 ensure it does not cause Accenture, through any intentional act or omission, to be in breach of any Data Privacy Laws;

4.1.2 Process Accenture Personal Data only on the written instructions of Accenture, or to the extent reasonably necessary for the performance of the Agreement, or as required by applicable law. Provider shall not collect, retain, use, disclose, or otherwise Process Accenture Personal Data for any other purpose. Provider shall not sell Accenture Personal Data in any circumstances. Provider hereby certifies that it understands and complies with the restrictions in this Section 4.1.2 and will issue this certification to Accenture and/or Client upon reasonable request by Accenture;

4.1.3 take reasonable steps to inform its personnel, and any other person acting under its supervision, of the responsibilities of any Data Privacy Laws due to access to Accenture Personal Data, and ensure the reliability of such persons who may come into contact with, access or Process Accenture Personal Data;

4.1.4 provide full cooperation and assistance to Accenture in ensuring that requests from and the legal rights of individuals to whom Accenture Personal Data relates are appropriately addressed without undue delay, including the rights of subject access, rectification, erasure, portability, and the right to restrict or object to certain Processing;

4.1.5 notify Accenture promptly if Provider is required by law, court order, warrant, subpoena, or other legal process to disclose any Accenture Personal Data to any person other than Accenture, the relevant Accenture client, or another sub-processor of Accenture expressly approved in writing by Accenture to receive such information, unless prohibited by applicable law from notifying Accenture. Unless prohibited by applicable law, Provider will (a) promptly notify Accenture prior to such disclosure; (b) cooperate with Accenture in the event that Accenture elects to legally contest such disclosure, ensure confidential treatment of such information, or otherwise attempt to avoid or limit such disclosure; and (c) limit such disclosure to the extent legally permissible;

4.1.6 make all reasonable efforts to ensure that Accenture Personal Data is accurate and up-to-date at all times, while in its custody or under its control, to the extent Provider has the ability to do so;

4.1.7 provide Accenture with all information necessary to demonstrate Provider's (or Provider's Sub-processors') compliance with this Data Privacy Schedule, Data Privacy Laws and Information Security Obligations;

4.1.8 permit Accenture, or its duly authorized representatives, on reasonable prior notice, to inspect and/or audit the Provider's (and Provider's Sub-processors') Processing activities that are relevant to the Processing of Accenture Personal Data, to verify that Provider's (and Provider's Sub-processors') data processing activities related to Accenture Personal Data are in compliance with the Agreement (including its Schedules), Accenture's written instructions and Data Privacy Laws. Provider shall allow for and contribute to audits, including inspections, conducted by Accenture or another auditor mandated by Accenture;

4.1.9 notify Accenture immediately in writing (i) if in Provider´s opinion, Accenture´s instructions or the terms of the Agreement breach Data Privacy Laws; and/or (ii) of any investigation, litigation, arbitrated matter or other dispute relating to Provider's (or Provider's Sub-processors') information security or privacy practices;

4.1.10 reasonably cooperate with Accenture in designing a remedial response to implement new requirements required by any changes in Data Privacy Laws applicable to Accenture Personal Data, (including new physical, technical, organizational, security, or data privacy measures).

4.2 **Sub-processors.** Provider shall not engage a Sub-processor with respect to any Processing of Accenture Personal Data without Accenture´s prior written approval, in which case Provider and the applicable Sub-processor(s) must be bound by a written agreement that includes the same data protection obligations on the Sub-processor(s) as set out in this Data Privacy Schedule and make a copy of such agreement(s) available to Accenture upon its request. Provider will remain fully liable to Accenture for any act or omission of any Sub-processor in the performance of that Sub-processor´s obligations. Instructions given by Provider to any Sub-processor must be in furtherance of instructions provided by Accenture to Provider. If Provider (or any Sub-processor) cannot comply with Accenture's instructions or this Data Privacy Schedule, Provider shall promptly notify Accenture in writing of such inability to comply, in which case Accenture is entitled to suspend the transfer of Personal Data.

4.3 **Cooperation.** Provider shall fully assist and cooperate with Accenture and its clients in ensuring their compliance with Data Privacy Laws. If Accenture needs to provide information (including details of Provider's services) to a supervisory authority (whether directly or indirectly via an Accenture client), Provider shall assist Accenture in providing such information, to the

extent that such information is solely in the possession of the Provider or its Sub-processors.

4.4 **Remedies.** Provider agrees that, in the event of a breach of this Data Privacy Schedule, neither Accenture nor any affected Accenture client(s) will have an adequate remedy in damages. Therefore, Accenture or any affected Accenture client(s) shall be entitled to seek injunctive or equitable relief, to immediately cease or prevent the Processing, use or disclosure of Accenture Personal Data not contemplated by the Agreement, and/or to enforce the terms of the Agreement (including this Data Privacy Schedule), and/or to ensure compliance with any Data Privacy Laws. Provider shall indemnify Accenture against any loss, liability, cost damage and expense incurred as a result of a breach by the Provider or its agents or Sub-processors of this Data Privacy Schedule.

5. PROVIDER PERSONAL DATA

Accenture may receive Personal Data regarding Provider's employees, directors and other personnel, as part of maintaining its business relationships with Provider under the Agreement. Personal Data may be obtained by Accenture indirectly through internal security systems or other means. Accenture is hereby permitted, and Provider herby authorizes Accenture, to process such Personal Data for purposes related to the Agreement and for relevant purposes under Accenture's global Data Privacy Policy (a copy of which will be made available by Accenture to Provider upon request) and the Accenture Privacy Statement at www.accenture.com/us-en/privacy-policy. For such purposes, Accenture may transfer such Personal Data to any country where Accenture's global organization and its clients and vendors operate. If required by Data Privacy Laws, Accenture and Provider agree to sign any additional agreement or amendment that may be required to allow transferring such Personal Data outside its jurisdiction of origin pursuant to such Data Privacy Laws.

ANNEX B

INFORMATION SECURITY GUIDELINES

SCHEDULE X

This information security schedule, including any attachment hereto, ("**Information Security Schedule**") is subject to the terms and conditions of the Agreement. For the purposes of this Information Security Schedule, **"Provider"** shall mean [**INSERT NAME USED IN THE AGREEMENT FOR SUPPLIER/VENDOR**] and its third-party providers/suppliers/agents and subcontractors, and "**Accenture**" shall mean [**INSERT NAME USED FOR ACCENTURE CONTRACTING ENTITY IN THE AGREEMENT**]. Terms not defined herein shall have the meaning set forth in the Agreement. In the event of a conflict between the Agreement and this Information Security Schedule, this Information Security Schedule shall prevail.

1. INFORMATION SECURITY REQUIREMENTS

1.1 Where Provider knows, or reasonably suspects, an accidental or unauthorized loss, destruction, acquisition, disclosure, access, manipulation, use or other form of compromise of Accenture Data (a "**Security Incident**") has occurred, Provider will notify Accenture's point of contact in writing promptly, and in any event within forty-eight (48) hours, or as prescribed by laws/regulations, following such discovery and cooperate with Accenture in any breach investigation or remediation efforts. If Accenture notifies Provider of a security vulnerability or incident that is identified by Accenture or a third-party to Accenture, Provider will, in good faith, address the security vulnerability or incident as required in this Information Security Schedule and the Accenture Information Security Requirements (found at https://www.accenture.com/us-en/about/legal/information-security-supplier-security-requirements). For the purposes of this Information Security Schedule: (i) **"Accenture Data"** shall mean Buyer data or have the meaning set forth in the Agreement, or if no term is defined, then **"Accenture Data"** shall mean all information or data collected, stored, processed, received and/or generated by Provider in connection with providing the applicable Provider Services to Accenture and (ii) **"Provider Services"** shall mean the Technology and the Professional Services or have the meaning set forth in the Agreement and also includes any other services provided by the Provider under the Agreement, and shall include any software and equipment provided by Provider (including third party software and equipment) required to access the Provider Services or provide the Provider Services.

1.2 Provider represents and warrants that it shall implement appropriate technical and organizational security measures, based on current Industry Standards. **"Industry Standards"** means commercially reasonable security measures in all applicable equipment, software systems, services and platforms that Provider uses to access, process and/or store Accenture Data, that are designed to ensure the security, integrity, and confidentiality of Accenture Data, and to protect against any Security Incident(s) or any other unauthorized disclosure of Accenture Data, including those safeguards, practices and procedures prescribed **in at least one of the following**:

(i) ISO / IEC 27000-series – see https://www.iso.org/isoiec-27001-information-security.html; and/or
(ii) COBIT 5 – http://www.isaca.org/cobit/; and/or
(iii) Cyber Security Framework – see http://www.nist.gov/cyberframework/; and/or
(iv) Secure Software Development Framework – see https://csrc.nist.gov/publications/detail/sp/800-218/final; and/or
(v) Center for Internet Security Controls – see https://www.cisecurity.org/; and/or
(vi) When credit card data is stored, access, viewed or processed: Payment Card Industry Data Security Standards (**"PCI DSS"**) – see http://www.pcisecuritystandards.org/; and/or
(vii) When "Protected Health Information" is stored, accessed, viewed, or processed: Health Insurance and Portability Accountability Act (**"HIPAA"**)**:** http://www.hhs.gov/hipaa/.

Further, Provider represents and warrants it will comply with applicable laws and regulatory requirements to ensure that Accenture Data is not destroyed (except as expressly permitted under this Agreement), lost, altered corrupted or otherwise impacted such that it is not readily usable. Upon Accenture's request, Accenture Data shall be immediately provided or otherwise made accessible to Accenture by Provider, either, at Accenture's option, using the Provider Services or in an Industry Standard format specified by Accenture.

Provider also represents and warrants that it currently has, and shall maintain in effect, for the term of the Agreement and all Orders, the security methods, practices, and other related requirements stated in this Information Security Schedule as may be reasonably modified from time-to-time by Accenture upon notice to Provider.

1.3 Illicit Code. Except for the functions and features expressly disclosed in Provider's documentation provided or made available to Accenture, Provider represents and warrants that the Provider Services, deliverables, and software and equipment that process, store or transmit Accenture Data do not and will not knowingly contain any malicious code, including, but not limited to, viruses, malware, worms, malicious backdoors, date/time bombs, ransomware, spyware, rogue software, trojan horses or any disabling code.

1.4 Security of All Software Components. Provider agrees to appropriately inventory (aka, Software Bill of Materials) all software components (including, but not limited to, open-source software) used in the Provider Services, software, equipment and/or deliverables. Provider will assess whether any such software components have any security defects and/or vulnerabilities that could lead to a Security Incident. Provider shall perform such assessment and remediate identified security defects or vulnerabilities prior to delivery of, or providing access to, such software components to Accenture and on an on-going basis thereafter during the term of the Agreement and any Orders and Statements of Work under the Agreement. Provider further agrees not to disclose the existence of this Agreement, nor any Accenture Data or intellectual property of Accenture, in connection with any remediation efforts (including, for example, contribution of code to an open-source software project).

1.5 Source Code Protection. Provider shall protect source code from various security risks, including outsider and insider threats. Provider will implement a layered security approach such as, but not limited to a) defining a set of rules, requirements, and procedures for handling and protecting code, b) use source code security analysis tools, such as Static Application Security Testing (SAST), to detect security flaws and other issues during development, c) define who is allowed to access source code, codebase and source code repositories, d) encrypt confidential and sensitive data both in transit and at rest, e) implement network security solutions such as firewalls, Virtual Private Networks (VPN), anti-virus, and anti-malware software as basic protections, f) secure the endpoints or entry points of end-user devices with endpoint security software, and g) ensure that all concepts and inventions related to software are protected by copyright law and necessary patents.

1.6 Resiliency. During the term of the Agreement and all Orders and Statements of Work under the Agreement, Provider shall maintain a high availability ("**HA**") solution and related plan that is consistent with Industry Standards for the Provider Services being provided. The HA solution is required to have a highly available technical architecture across all the application tiers (e.g., Web, application, database, etc.) with nodes deployed across different physical data centers (e.g., across AWS Availability Zones) with no more than one (1) hour of recovery time and data loss. If an HA solution is not able to be deployed, Provider shall maintain a disaster recovery ("**DR**") solution and related plan that is consistent with Industry Standards for the Provider Services being provided. The DR solution will ensure identified critical capabilities are restored within a twenty-four (24)-hour period with no more than twelve (12) hours of data loss in the event of a declared disaster or major system outage. Provider will test the HA or DR solution and related plan at least twice annually or more frequently if test results indicate that critical systems were not capable of being recovered within the periods above. Provider will provide summary test results for each exercise which will include the actual recovery point (how much data lost, if any) and recovery times (time to bring back applications and/or the Provider Services, if not automated failover) achieved within the exercise. Provider will provide agreed upon action plans to promptly address and resolve any deficiencies, concerns, or issues that may prevent the critical functionality of the application and/or Provider Services from being recovered within twenty-four (24) hours in the event of a disaster or major system outage. Further, Provider will notify Accenture, in a timely manner, when Provider initiates Provider's business continuity plan.

2. SECURITY ASSESSMENT

2.1 Security Assessment. If Accenture reasonably determines, or in good faith believes, that Provider's security practices and procedures do not meet Provider's obligations pursuant to the Agreement or this Information Security Schedule, then Accenture may notify Provider of the deficiencies. Provider shall without unreasonable delay (i) correct such deficiencies at its own expense and (ii) permit Accenture, or its duly authorized representatives, on reasonable prior notice, to assess Provider's and Provider subcontractors' security-related activities that are relevant to the Agreement. Further, (A) Provider will complete, in a timely and accurate manner, an information security questionnaire provided by Accenture to Provider, on an annual basis or more frequently upon Accenture's request, in order to verify Provider's and its subcontractors' compliance its security-related obligations in the Agreement and (B), if the Provider is providing any managed infrastructure, cloud (e.g. Iaas), vulnerability or security services as part of the Provider Services to Accenture or its client, Provider agrees to undergo an assessment of such

Provider Services and related deliverables and Provider will provide evidence that the agreed upon Provider Services are meeting the security requirements and/or specific Accenture client requirements for the Provider Services (each a "Security Assessment").

2.2 Security Issues and Remediation Plan. Security issues identified by Accenture during a Security Assessment will have an assigned risk rating and an a mutually agreed upon timeframe to remediate. Provider shall remediate all security issues identified within the agreed remediation timeframes and failure to comply will result in Accenture having the right to terminate this Agreement without the payment of any early termination fee and with the right to a refund of any prepaid amounts for the period of time after the effective date of such termination.

3. CONTROL AUDIT RIGHTS

SSAE18 SOC2 Reports

During each calendar year, Provider will provide, at Provider's cost, a SSAE18 SOC2 Type II report for identified locations and Provider Services, covering information security management implementation and operating effectiveness, that are used by Provider to develop software or deliver the Provider Services, conducted by an internationally recognized independent public accounting firm. The minimum scope of these reports will be the Trust Service Principles of Security (also known as the Common Criteria) and Availability. Provider will comply with future guidance relating to SSAE18 as issued by the AICPA, IAASB, the Securities and Exchange Commission or the Public Company Accounting Oversight Board.

If Provider requests that Provider Services or the development of software, which in Accenture's reasonable opinion are required to be provided from a location covered by a SSAE18 SOC 2 report described above, be provided from a location not covered by a SSAE18 SOC2 report, the parties will address how to meet such requirement prior to the Provider Services being provided from such location.

Where the SSAE18 SOC2 Type II report is not available, Provider shall provide, if available and upon request, any recent copy of its annual audit report, covering information security management implementation and operating effectiveness of systems.

SSAE18 SOC1 Reports

During each calendar year, if available, Provider will provide, at Provider's cost, SSAE18 SOC1 reports for identified locations that are common Provider centers (i.e., service centers from which services are provided to multiple clients) conducted by an internationally recognized independent public accounting firm. The scope of these reports will be the common controls that support multiple clients served from Provider centers. The coverage period of such reviews will cover at least nine months of Customer's fiscal year and be made available to Accenture by September 30th of each year, or with a different coverage period and delivery date as mutually agreed to by both the Provider and Accenture. Provider will provide Accenture a representation letter (otherwise referred to as a "bridge letter") in relation to the time period which is not covered by the reports. Provider will comply with future guidance relating to SSAE18 as issued by the AICPA, IAASB, the Securities and Exchange Commission or the Public Company Accounting Oversight Board.
Other than in connection with the provision of Services pursuant to a Accenture-approved business continuity and / or disaster recovery assistance plan, if either party requests that Services, which in Provider's reasonable opinion are required to be provided from a location covered by an SSAE18 SOC1 report described above, be provided from a location not covered by an SSAE18 SOC1 report, the parties will address how to meet such requirement prior to the Services being provided from such location.
Customer, at its own expense, may audit Provider (either at Provider's facilities or that portion of Provider's center from which Services are provided to Customer). Provider will permit Customer, or its duly authorized representatives, on reasonable prior notice, to assess Provider's and its Provider agents' activities that are relevant to this section. If Customer requests a Customer specific SSAE18 SOC1 report, Provider will contract with an internationally or nationally recognized independent public accounting firm to perform the Customer specific audit. Customer will be responsible for all costs associated with the Customer specific audit. Customer will be able to set the scope which shall be reasonably related to the Services and those portions of the Provider locations from which Services will be provided to Customer, establish the control objectives, determine the frequency of such audit, and determine the reporting period.

SUPPLEMENTARY MEASURES. In addition, in accordance with regulatory guidance following the European Court of Justice "Schrems II" decision, Provider further commits to maintaining the following additional technical, organizational and legal/contractual measures with respect to Accenture Data, including personal data.

Technical Supplementary Measures:

Accenture Data in transit between Provider entities will be strongly encrypted with encryption that:

- **a.** is state of the art,
- **b.** secures the confidentiality for the required time period,
- **c.** is implemented by properly maintained software,
- **d.** is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and
- **e.** does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.

Accenture Data at rest and stored by any Provider entities will be strongly encrypted with encryption that:

- **a.** is state of the art,
- **b.** secures the confidentiality for the required time period,
- **c.** is implemented by properly maintained software,
- **d.** is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and
- **e.** does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.

ACCENTURE INFORMATION SECURITY SUPPLIER SECURITY REQUIREMENTS

Provider agrees it has implemented and will maintain throughout the term of the Agreement and all Orders and Statements of Work the following technical and organizational measures, controls, and information security practices:

2. Information Security Policies

- **a. Policies for Information Security.** Provider's policies for information security shall be documented by Provider, approved by Provider's management, published, and communicated to Provider's personnel, contractors, agents and relevant external third parties.
- **b. Review of the Policies for Information Security.** Provider information security policies shall be reviewed by Provider at least annually, or promptly after material changes to the policies occur, to confirm applicability and effectiveness.
- **c. Information Security Reviews.** The Provider's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

3. Organization of Information Security

- **a. Security Accountability.** Provider shall assign one or more security officers who will be responsible for coordinating and monitoring Provider's information security function, policies, and procedures.
- **b. Security Roles and Responsibility**. Provider personnel, contractors and agents who are involved in providing Provider Services shall be subject to confidentiality agreements with Provider.
- **c. Risk Management**. Appropriate information security risk assessments shall be performed by Provider as part of an ongoing risk governance program that is established with the objective to recognize risk; to assess the impact of risk; and where risk reducing or mitigation strategies are identified and implemented, to effectively manage the risk with recognition that the threat landscape constantly changes.

4. Human Resource Security

- **a. Security Training.** Appropriate security awareness, education and training shall be provided to all Provider personnel and contractors.

5. Asset Management

- **a. Asset Inventory.** Provider shall maintain an asset inventory of all media and equipment where Accenture Data is stored. Access to such media and equipment shall be restricted to authorized personnel of Provider. Provider will ensure that no software or hardware that is past its End of Life (EOL) will be used in the scope of Provider Services without a mutually agreed risk management process for such items.
- **b. Asset Handling**
  - i. Provider shall classify Accenture Data so that it is properly identified and access to Accenture Data shall be appropriately restricted.
  - ii. Provider shall maintain an acceptable use policy with restrictions on printing Accenture Data and procedures for appropriately disposing of printed materials that contain Accenture Data when such data is no longer needed to provide the Provider Services under the Agreement.
  - iii. Provider shall maintain an appropriate approval process whereby such approval is provided to personnel, contractors, and agents prior to storing Accenture Data on portable devices; remotely accessing Accenture Data; or processing such data outside of Provider facilities. If storing Accenture Data on portable devices is approved and granted, Provider shall enforce the use of current Industry Standard encryption on the portable device. If mobile devices are used to access or store Accenture Data, Provider personnel, contractors and agents shall use a mobile device management (MDM)/mobile application mangement (MAM) solution that enforces encryption, passcode, and remote wipe settings to secure Accenture Data. Provider will prohibit the enrollment of mobile devices that have been "jail broken."

6. **Access Control.** Provider shall maintain an appropriate access control policy that is designed to restrict access to Accenture Data and Provider assets to authorized personnel, agents, and contractors.
   a. **Authorization**
      i. Provider shall maintain user account creation and deletion procedures for granting and revoking access to all assets, Accenture Data, and all internal applications while providing Provider Services under the Agreement. The Provider will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.
      ii. Provider shall maintain and update records of personnel who are authorized to access Provider systems that are involved in providing Provider Services and review such records at least quarterly.
      iii. Provider shall ensure the uniqueness of user accounts and passwords for each individual. Individual user accounts must not be shared.
      iv. Provider shall remove access rights to assets that store Accenture Data for personnel, contractors and agents upon termination of their employment, contract or agreement within two (2) business days, or access shall be appropriately adjusted upon change (e.g., change of personnel role).
      v. Provider will perform periodic access reviews for system users at least quarterly for all supporting systems requiring access control.
   b. **Least Privilege Access**
      i. Provider shall restrict access to Provider systems involved in providing Provider Services, to only those individuals who require such access to perform their duties using the principle of least privilege access.
      ii. Administrative and technical support personnel, agents or contractors shall only be permitted to have access to such data when required.
      iii. Provider shall support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., programming/administrator, developer/operations).
   c. **Authentication**
      i. Provider will use current, and at a minimum, Industry Standard capabilities to identify and authenticate personnel, agents and contractors who attempt to access information systems and assets.
      ii. Provider shall maintain current Industry Standard practices to deactivate passwords that have been corrupted or disclosed.
      iii. Provider shall monitor for repeated access attempts to information systems and assets.
      iv. Provider shall maintain current Industry Standard password protection practices that are designed and in effect to maintain the confidentiality and integrity of passwords generated, assigned, distributed, and stored in any form.
      v. Provider shall provide an Industry Standards based single sign-on (SSO) capability (SAML, Open Authorization (Oauth v2), etc.) which will support integration with Accenture's SSO solutions to enable authentication to access any Provider web-based application(s) provided as part of the Provider Services, unless the requirement is explicitly waived by Accenture. Details of how the single sign-on integration must be implemented are available from Accenture upon request. If SSO is not implemented due to technical limitations or Accenture requirements, multi-factor authentication will be required for access to all Provider application(s) and infrastructure provided as part of the Provider Services.
      vi. Provider shall maintain and enforce a password policy that is aligned to current Industry Standards (e.g., NIST Cyber Security Framework, PCI DSS (Payment Card Industry Data Security Standard), Center for Internet Security) and default passwords must be changed before deploying any new asset. In the event that Provider Services includes the management of Accenture or its client infrastructure and environments, account lockout thresholds must be consistent with Accenture or its client account lockout standards, whichever is most strict.
      vii. Provider personnel, agents and contractors shall use multi-factor authentication and encrypted sessions for access to Provider systems. In the event that Provider Services require external connections to Accenture or Accenture client project dedicated environments, Accenture must provide approval of the connections.

7. **Cryptography.** Provider shall maintain policies and standards regarding the use of cryptographic controls that are implemented to protect Accenture Data. Provider shall implement Industry Standard key management policies and practices designed to protect and generate encryption keys for their entire lifetime.

8. **Physical and Environmental Security**

a. **Physical Access to Facilities.** Provider shall limit access to facilities (where systems that are involved in providing the Provider Services are located) to identified personnel, agents and contractors.
b. **Physical Access to Components.** Provider shall maintain records of incoming and outgoing media containing Accenture Data, including the type of media, the authorized sender/recipient, the date and time, the number of media, and the type of data the media contains. Provider shall ensure that backups (including remote and cloud service backups) are properly protected via physical security or encryption when stored, as well as when they are moved across the network. In the event that backup media of Accenture and/or Accenture client data is stored / shipped offsite, Accenture must provide approval of the storage location.
c. **Protection from Disruptions.** The Provider shall protect equipment from power failures and other disruptions caused by failures in supporting utilities. Telecommunications and network cabling must be protected from interception, interference, and/or damage.
d. **Secure Disposal or Reuse of Equipment.** Provider shall verify equipment containing storage media, to confirm that all Accenture Data has been deleted or securely overwritten using Industry Standard processes, prior to disposal or re-use.
e. **Clear Desk and Clear Screen Policy**. Provider shall adopt a clear desk policy for papers and removable storage media and a clear screen policy.

9. **Operations Security**
   a. **Operations Policy.** Provider shall maintain appropriate operational and security operating procedures and such procedures shall be made available to all personnel who require them.
   b. **Logging and Monitoring of Events**
      i. Provider must enable logging and monitoring on all operating systems, databases, applications, and security and network devices that are involved in providing Provider Services. Logs must be kept for a minimum of 6 months or as long as legally required, whichever is longer. Logs must capture the access ID, the authorization granted or denied, the date and time, the relevant activity, and be regularly reviewed. All relevant information processing systems shall synchronize time to a single reference time source.
      ii. Logging capabilities shall be protected from alteration and unauthorized access.
   c. **Protections from Malware.** Provider shall maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks. Provider shall maintain software at the then current major release for Provider owned anti-malware software and shall maintain appropriate maintenance and support for new releases and versions of such software.
   d. **Encrypted Backup**. Provider shall maintain an encrypted backup and restoration policy that also protects Accenture Data from exposure to ransomware attacks, and shall back up Accenture Data, software, and system images in accordance with Provider policy unless other such requirements are agreed upon. Provider shall regularly test restoration procedures.
   e. **Control of Software and Utilities.** Provider shall enforce policies and procedures that govern the installation of software and utilities by personnel.
   f. **Change Management.** Provider shall maintain and implement procedures to ensure that only approved and secure versions of code, configurations, systems, utilities, and applications will be deployed for use.
   g. **Encryption of Data at Rest**. Provider shall encrypt data at rest, including data at rest in cloud instances and storage buckets, using current Industry Standard encryption solutions or shall provide the capability with instructions to Accenture so that Accenture may enable further encryption, at Accenture's discretion.

10. **Communications Security**
    a. **Information Transfer and Storage.**
       i. Provider shall use current Industry Standard encryption, TLS (Transport Layer Security) minimum version 1.2, to encrypt Accenture Data that is in transit.
       ii. Provider shall use TLS, minimum version 1.2, over SMTP (Simple Mail Transfer Protocol) when exchanging emails as a standard practice to encrypt emails in transit.
       iii. Provider shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy of reject to lower the chance of spoofed or modified emails from valid domains. This is required for email that is sent from Provider applications.
       iv. In the event that Provider Services include the management of Accenture client email systems, such systems must be configured and implemented to agreed-upon standards.

v. Provider shall utilize a secure collaboration platform that is enabled to restrict access and encrypt communications and Accenture Data.
vi. Provider shall restrict access through encryption to Accenture Data stored on media that is physically transported from Provider facilities.

b. Security of Network Services. Provider shall ensure that Industry Standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced. In the event that Provider Services include the management of network services and components owned by Accenture or its client, such services and components must be configured and implemented to agreed-upon standards.

c. Intrusion Detection. Provider shall deploy intrusion detection and intrusion prevention systems to provide continuous surveillance for intercepting and responding to security events as they are identified and update the signature database as soon as new releases become available for commercial distribution.

d. Firewalls. Provider shall have appropriate firewalls in place which will only allow documented and approved ports and services to be used. All other ports will be in a deny all mode.

e. Web Filtering. Provider shall have a Web filtering policy in place to control the content that users can access over the Internet. This includes restricting the use of personal emails and file sharing sites.

f. Data Loss Prevention. Provider shall have a data loss prevention policy in place to monitor for or restrict the unauthorized movement of Accenture Data.

11. System Acquisition, Development and Maintenance

a. Workstation Encryption. Provider will require Industry Standard full disk encryption on all workstations and/or laptops used by personnel, contractors and agents where such personnel are accessing or processing Accenture Data.

b. Application Hardening.

i. Provider will maintain and implement secure application development policies, procedures, and standards that are aligned to Industry Standard practices such as the SANS Top 25 Software Errors, the OWASP Top Ten project and the NIST Secure Software Development Framework (SSDF). This applies to web application, mobile application, embedded software, and firmware development as appropriate.
ii. All personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Provider Services and receive appropriate training regarding Provider's secure application development practices.

c. System Configuration and Hardening.

i. Provider will establish and ensure the use of Industry Standard secure configurations of technology infrastructure. Images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated on a regular basis to update their security configuration as appropriate.
ii. Provider will perform periodic access reviews for system administrators at least quarterly for all supporting systems requiring access control.
iii. Provider will implement patching tools and processes for operating systems and applications installed on the system. Provider shall have a defined process to remediate findings and will ensure that emergency/critical issues are addressed urgently and as soon as practicable within fourteen (14) days; high-risk issues are addressed within thirty (30) days; and medium-risk issues are addressed within ninety (90) days. When outdated systems can no longer be patched, Provider will update to the latest supported version of the operating system and applications installed on the system. If this is not possible, Provider shall purchase extended support and notify Accenture so that an appropriate risk assessment can be conducted. Provider will remove outdated, older, and unused software from the system. In the event that Provider Services include patch management for operating systems and applications owned by Accenture or its client, Provider shall document and implement an appropriate patching plan that includes agreed-upon remediation service level obligations.
iv. Provider will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

d. Infrastructure Vulnerability Scanning. Provider shall use Industry Standard and up-to-date products to scan its internal and external environment (e.g., servers, network devices, etc.) related to Provider Services on a quarterly basis. Provider shall have a defined process to remediate findings and will ensure that emergency/critical issues are addressed urgently and as soon as practicable within fourteen (14) days; high-risk issues are addressed within thirty (30) days; and medium-risk issues are addressed within ninety (90) days. In the event that Provider Services include infrastructure

vulnerability management for infrastructure owned by Accenture or its client, Provider shall document and implement an infrastructure scanning and vulnerability remediation plan that is to be approved by Accenture.

e. **Application Vulnerability Assessment.** Provider will perform application security vulnerability assessments prior to any release and on a recurring basis. The assessments must cover all web application, mobile application, stand-alone application, embedded software, and firmware vulnerabilities defined by the Open Web Application Security Project (OWASP) or those listed in the SANS Top 25 Software Errors or its successor current at the time of the test. Provider will ensure all critical and high-risk vulnerabilities are remediated prior to release. On a recurring basis, Provider shall ensure that emergency/critical vulnerabilities are addressed urgently and as soon as practicable within fourteen (14) days; high-risk vulnerabilities are addressed within thirty (30) days; and medium-risk vulnerabilities are addressed within ninety (90) days. This applies to web application, mobile application, stand-alone application, embedded software, and firmware development as appropriate to the Agreement. In the event that Provider Services include application vulnerability management for applications owned by Accenture or its client, Provider shall document and implement an application vulnerability assessment and remediation plan that is to be approved by Accenture.

f. **Penetration Tests and Security Evaluations of Websites.** Provider shall use an established Industry Standard program to perform external and internal penetration tests and security evaluations of all systems and websites involved in providing Provider Services prior to use and on a recurring basis no less frequently than once in a twelve (12)-month period. Provider shall have a defined process to remediate findings and will ensure that emergency/critical issues are addressed urgently and as soon as practicable within fourteen (14) days; high-risk vulnerabilities are addressed within thirty (30) days; and medium-risk issues are addressed within ninety (90) days.

g. **Supporting Documentation.** Upon Accenture request, Provider shall provide a summary of vulnerability scans, penetration tests and/or any security evaluations conducted, including any open remediation points. In the absence of such summaries, documentation sufficient to prove that such scans have been conducted shall be provided.

h. **Separation of Environments.** Provider shall maintain separate environments for production and non-production systems and developers should not have unmonitored access to production environments.

12. Provider Relationships

a. Where other third-party applications or services must be engaged by Provider, Provider's contract with any third-party must clearly state appropriate security requirements substantially similar to this Information Security Schedule. In addition, service level agreements with the third party must be clearly defined.

b. Any external third-party or resources gaining access to systems must be covered by a signed agreement containing confidentiality language consistent with the confidentiality and security requirements of the Agreement.

c. Provider shall regularly conduct security reviews of third-party suppliers to address physical and logical security requirements, privacy protection, breach reporting, and contractual requirements. Provider shall ensure that all findings from such security reviews are promptly remediated.

d. Provider will perform quality control and security management oversight of outsourced software development.

13. Information Security Incident Management

a. Incident Response Process

i. Provider shall maintain a record of Security Incidents noting the description of the Security Incident, the applicable time periods, the impact, the person reporting and to whom the Security Incident was reported, and the procedures to remediate the incident.

ii. In the event of a Security Incident identified by Provider, Accenture, or other third party, Provider will: (a) promptly investigate the Security Incident; (b) promptly provide Accenture with all relevant detailed information as reasonably requested by Accenture about the Security Incident; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

iii. The Provider shall track disclosures of Accenture Data, including what type of data was disclosed, to whom, and the time of the disclosure.

14. Compliance

a. **Legal and Contractual Requirements.** Provisions regarding compliance with laws, intellectual property and data privacy are contained in the body of the Agreement and applicable schedules.

ANNEX C

INVOICE RECEIVING CHANNEL

Accenture Suppliers	Accenture Business Services, Inc. Suppliers
Manila Vendors RTP Drop Box Ground Floor Cybergate Tower 2, Pioneer Street, Mandaluyong City Monday – Friday, 8:00am – 5:00pm **Cebu Vendors** RTP Drop Box 14th Floor Reception Area eBloc2 IT Park Lahug Apas Cebu City Cebu Philippines 6000 Monday – Friday, 8:00am – 5:00pm **Ilocos Vendors** Courier Invoice to: 9.48 Mailroom Cybergate Tower 1, Pioneer Street, Mandaluyong City, Philippines Monday – Friday, 8:00am – 5:00pm **Foreign Vendors, CAS Invoice (Fieldglass, IQN, T360)** • You can send electronic invoices to acn.inv.manilaph@accenture.com. Kindly observe below guidelines: - Generation of unique reference (URN) is per attachment so make sure to attach invoice and any supporting documents e.g. PO copy, Delivery Receipt, email approval and etc. in one attachment as zipped file. - You can send multiple invoices in one email, just separately attach the invoices plus supporting documents in separate zipped files so the system will generate unique reference per attachment - These are the only allowed file types: DOC, .DOCX, .PDF, .TIF, .TIFF, .XLS, .XLSX, .ZIP, .RAR - The acn.inv.manilaph@accenture.com email id is for invoice submission only and queries to that email address will go unattended. All queries regarding your submission should be addressed only to PhilsDC.Vendors@accenture.com. **CAS Invoice (SAP RE-FX)** • You can send electronic invoices to acn.ph.lease.invoice@accenture.com.	**Manila Vendors** RTP Drop Box Ground Floor Cybergate Tower 2, Pioneer Street, Mandaluyong City Monday – Friday, 8:00am – 5:00pm **Foreign Vendors, CAS Invoice (Fieldglass, IQN, T360)** • You can send electronic invoices to absi.philippines.inv@accenture.com. Kindly observe below guidelines: - Generation of unique reference (URN) is per attachment so make sure to attach invoice and any supporting documents e.g. PO copy, Delivery Receipt, email approval and etc. in one attachment as zipped file. - You can send multiple invoices in one email, just separately attach the invoices plus supporting documents in separate zipped files so the system will generate unique reference per attachment - These are the only allowed file types: DOC, .DOCX, .PDF, .TIF, .TIFF, .XLS, .XLSX, .ZIP, .RAR The absi.philippines.inv.@accenture.com email id is for invoice submission only and queries to that email address will go unattended. All queries regarding your submission should be addressed only to PhilsDC.Vendors@accenture.com. **CAS Invoice (SAP RE-FX)** • You can send electronic invoices to acn.ph.lease.invoice@accenture.com.