CONFORMITY NORMS

MADAM, SIR,

Accenture has a longstanding commitment to manage its business relationships responsibly. This commitment to act in accordance with the highest ethical standards is part of its core values.

Integrity and compliance with laws are key conditions for Accenture in conducting its business. In this context, Accenture has selected you as a supplier / Provider which means that you warrant to strictly respect ethics and comply with the regulations in force. By agreeing to deliver goods and / or provide services (the "**Provider Offerings**") to Accenture as part of the Order:

- You agree to take commercially reasonable efforts to materially adhere to the "Accenture Supplier Standards of Conduct" https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-58/accenture-supplier-standards-of-conduct-final-en.pdf
- You declare to be in conformity with the warranties listed in the Anti-Corruption Schedule.
- You declare that you comply with the technical and operational requirements specific to security as defined in the Information Security Schedule.
- You declare to be in compliance with the personal data obligations defined in the Data Privacy Schedule and the Standard Contractual Clauses in their newest version approved by the EC, Option 1.

These terms and conditions shall apply provided that there is no particular agreement which has been negotiated with you.

YOU WILL BE IDENTIFIED BELOW AS THE PROVIDER.

1. Determination of the Contracting Parties.

Accenture, the Client, is understood as Accenture S.A.S.U., Société par Actions Simplifié à associé Unique (SASU) / RCS Paris 732 075 312 / Capital: 17,250,911.00 EUR, having its registered office at 118-122 avenue de France, 75013 Paris, France or any Accenture Group entity duly identified in the contractual document.

The Accenture Group is defined herein as any company registered in France that is controlled within the meaning of the relevant legislation by Accenture.

You are identified below as the Provider, which is identified in the Purchase Order or ''PO''.

2. Compliance with Laws.

Each Party covenants to comply with all applicable laws, ordinances and regulations, including the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act, and all other applicable anti-corruption laws, anti-competition laws, and export compliance laws. The Provider will not knowingly as to the cause or intentionally, in consideration of Provider's professional capacity and of its compliance with French laws, structuring its obligations, take any action, or fail to take any action, that would result in Accenture or one of its Clients violating any such law, rule, ordinance or regulation.

Provider agrees to execute all the warranties, declarations and commitments defined in the Anti-Corruption Schedule.

Records and Audit Rights: Throughout the duration of the commercial relations with Accenture and for thirty-six(36) months thereafter, The Provider will retain and, upon reasonable notice, will provide Accenture reasonable access to audit its records relating to the Services performed in connection with performance of the Services, upon at least thirty (30) days-notice from Accenture. At the Provider'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 agree to an appropriate confidentiality or non-disclosure agreement. The Provider shall cooperate fully in any audit conducted by or on behalf of Accenture or of its Clients. Before the commencement of any such audit, Accenture and Provider shall mutually agree upon the scope, timing and duration of the audit in addition to the reimbursement rate for which Accenture shall be responsible. Any such audit performed herein is limited to once per every twelve (12) months, except if this would be a regulatory audit or demanded by a government authority, and be performed in a way to minimize disruptions to Provider's operations.

IF YOU DO NOT EXTEND THE WARRANTIES, DECLARATIONS AND COMMITMENTS OF THE ANTICORRUPTION SCHEDULE, PLEASE INDICATE THIS PRIOR TO THE BEGINNING OF THE SERVICES TO THE PROCUREMENT.SUPPORT@ACCENTURE.COM OR TO YOUR Accenture CONTACT (IDENTIFIED IN THE PO).

3. Information Security.

In the event that you provide Accenture with Services or supplies involving:

- ✓ a transfer, storage, or processing of personal data within the meaning of the laws on information and freedoms;
- ✓ a transfer, storage, or processing of sensitive data of Accenture or any of its Client;
- ✓ the supply of goods or equipment related to new technologies;

You agree to comply with the security-related technical and operational requirements as set out in Information Security Schedule which are essential and decisive of Accenture 's commitment.

IF YOU DO NOT AGREE TO THE INFORMATION SECURITY MEANS SET FORTH HEREIN, PLEASE INDICATE THIS PRIOR TO THE BEGINNING OF THE SERVICES TO THE PROCUREMENT.SUPPORT@ACCENTURE.COM OR TO YOUR Accenture CONTACT (AS IDENTIFIED IN THE PURCHASE ORDER).

4. Personal Data.

Provider undertakes to comply with the provisions of the French law "Informatique et Libertés" n ° 78-17 of 6 January 1978 and the general data protection framework and of the Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 (the "**General Data Protection Regulation**"), as they are required to deal with "Personal Data" within the meaning of the said standards in the context of performing the Agreement. The Provider essentially undertakes to process Accenture Data in accordance with a specific and legitimate purpose, fair and lawful collection, and relevant and not excessive data. The reciprocal commitments of the Parties in this regard are described in the Data Privacy Schedule.

The Provider is advised that Accenture implements a processing of personal data to manage its relations with its own Providers. The collected data is essential for such management and will be analyzed, processed and transmitted to relevant Accenture departments.
This data may be subject, for the communication of or operations involving such data, to a transfer to companies in the Accenture group, their subcontractors or Providers located in countries that may or may not benefit, as the case may be, from an adequate level of protection. Internal rules designed to organize the cross-border flow of intra-group personal data and agreements aimed at organizing the transfer of such data to third-party companies have been developed in order to ensure an adequate level of protection.
The right of information and access of the Provider's employees may be exercised by mail to the Procurement contact person, Accenture , accompanied by a copy of an identity document or by e-mail to the Accenture Data Privacy Officer at dataprivacy@accenture.com.

INSTRUCTIONS DOCUMENTS TO BE PROVIDED BY THE SERVICE PROVIDER /SUPPLIER/CONTRACTOR REGARDING THE LAWS ON ILLEGAL WORK

All these documents and declarations **must be drafted in French** or accompanied **by a translation in French**.
Affidavits and documents provided at the time of signing the sub-contracting agreement must be renewed every six months, until the end of execution of the agreement.
Please consider with attention the following note reminding your legal and contractual obligations toward Accenture.
Accenture designated PROVIGIS as collector of the following documents. Please fill in your supplier profile on:

Please insert the requested documents not forgetting the requested "**specific documents**"

SERVICE PROVIDER / SUPPLIER / CONTRACTOR BASED IN FRANCE (ARTICLE D 8222-5 OF THE LABOUR CODE AND D 243-15 OF THE SOCIAL SECURITY CODE)

1. An attestation for provision of social declarations and payment of social security allocations and contributions stipulated under Article L243-15 of the social security code of the URSSAF, which is less than six(6) months old.
2. A copy of the extract of registration in the Trade and Companies Register (KBIS).
3. Certificate of professional insurance.
4. In case of employment of foreign employees subject to work authorization (Article D8254-2 of the Labour Code): a list of names specifying, for each employee, his or her date of recruitment, nationality and the type and serial number of the permit equivalent to a work permit ("Liste nominative des travailleurs étrangers").

SERVICE PROVIDER / SUPPLIER / CONTRACTOR ESTABLISHED OR RESIDING ABROAD (ARTICLE D 8222-7 AND 8254-1 AND SEQ OF THE LABOUR CODE):

1. A document mentioning the intracommunity VAT number or, if not based in a country of the European Union, a document mentioning the identity and address of the representative with the French tax administration.
2. a) A document attesting the regularity of the social situation in regards to regulation (EC) No.883/2004 of 29 April 2004 or in regards to an international social security agreement. It may concern certificates of temporary employment abroad called "E101 or A1".
And, when the legislation of the country of residence requires it, a document issued by the organization managing the mandatory social regime and mentioning that your company is up-to-date with social declarations and payment of the related contributions, or an equivalent document.
b) In the absence of the documents mentioned in 2 a) above, an attestation for provision of the social declarations and payment of social security allowances and contributions stipulated under Article L243-15 of the social security code issued by the URSSAF.
3. When it is mandatory to be registered in a professional register in the country of establishment or domiciliation, a document issued by the authorities maintaining the professional register or an equivalent document certifying this registration.
4. A certificate of professional insurance.
5. In case of employment of foreign employees on the Accenture site, subject to the work permit (Article D8254-2 of the Labour Code): a list of names specifying, for each employee, his date of recruitment, nationality and the type and serial number of the permit equivalent to a work permit. This list must be mandatorily completed, if, during the execution on site, the sub-contractor decides to employ foreign personnel which had not been initially planned for, and which is subject to the work permit.
6. In case of employment of foreign employees on Accenture site (posting worker) : copy of the declaration of posting of workers in France (cerfa 13816-02)
https://entreprendre.service-public.fr/vosdroits/R42380
Copy of the mandate of representation of the Provider in France (cerfa 13816-02)
For complementary informations :
https://travail-emploi.gouv.fr/droit-du-travail/detachement-des-salaries-posting-of-employees/posting-of-employees/
and the guide created to the attention of foreign serive providers :
https://travail-emploi.gouv.fr/IMG/pdf/guide_mobilite_en_vf.pdf

DATA PRIVACY SCHEDULE

This data privacy schedule ("**Data Privacy Schedule**") is subject to the terms and conditions of the Agreement. This Data Privacy Schedule shall be considered a Schedule to the Agreement and shall be deemed part 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.

SECTION I - PROVIDER'S ROLE – DATA CONTROLLER

This Data Privacy Schedule – Section I - governs Provider's Processing of Accenture Personal Data where (a) Provider Processes Accenture Personal Data for its own commercial purposes; and (b) Provider does not Process Personal Data for or on behalf of Accenture; and (c) Provider will primarily (but not exclusively) obtain Personal Data directly from the applicable data subjects.
Provider as Data Controller shall (and shall ensure that its sub-processors shall):

1. Process Accenture Personal Data provided to Provider directly by Accenture only for the purposes contemplated by the Agreement;
   a. comply with Data Privacy Laws and any applicable to Provider's up to date Data Privacy Laws, policies and procedures relating to data privacy;
   b. obtain consent (where necessary) and/or provide notice to the data subject(s) in accordance with Data Privacy Laws, to enable execution the Agreement by Provider and Accenture and to provide Provider Offerings to data subjects and Accenture (if applicable);
   c. not Process and retain Accenture Personal Data for longer than is necessary for the performance of the Provider Offerings and/or the fulfilment of its obligations under the Agreement, or as required or permitted by applicable law, unless it is allowed to Process based on data subject(s) consent and in accordance with applicable laws;
   d. ensure that the international transfer of Personal Data (including any Personal Data which originates from a member state of the European Economic Area (EEA)) complies with Data Privacy Laws and shall enter into any additional agreement(s) and/or legally valid data transfer mechanism(s) required by Data Privacy Laws governing the access, Processing and international transfer of Personal Data;
   e. fully assist and cooperate with Accenture and its clients in their compliance with applicable security incident laws, including Article 33 of the GDPR. In particular, Provider
   f. 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.
   g. implement and maintain appropriate physical, technical and organisational security measures, in particular in such a manner (i) to ensure a level of security appropriate to the risk to the

Personal Data and (ii) to enable Provider (or any sub-processor of Provider) to fulfil its obligations, performed on Provider's cost, to respond to requests from data subjects exercising their rights under applicable Data Privacy Laws.

2. If Accenture needs to provide information (including details of the Provider Offerings provided by Provider) to a competent supervisory authority, Provider shall assist Accenture in providing such information, to the extent that such information is solely in the possession of the Provider.
3. The Parties shall provide full cooperation and assistance to each other in allowing the individual(s) to whom Personal Data relates (i) to have access to such Personal Data; and (ii) to ensure that such Personal data is deleted or corrected if such Personal Data is demonstrably incorrect. The Parties shall ensure that a record is kept of any requests by individuals to have information corrected.
4. The Parties agree to transfer Personal Data subject to the Standard Contractual Clauses, Module 1 (the "**Clauses**"), which are attached to this Data Privacy Schedule as Attachment B. In such cases, Accenture shall be the 'data exporter' and Provider shall be the 'data importer' as defined in the Clauses. For the purposes of Annex I to the Clauses, the following shall apply: (i) '**Data subjects**' are employees, contractors from both Parties; (ii) the '**Purpose of the transfer(s)**' is the performance of this Agreement (iii) the '**Categories of data**' are Personal Data Processed based on Section I; (iv) no sensitive data. Any changes to Clauses will be automatically incorporated to this Data Privacy Schedule; (v) Provider, hereby explicitly acknowledges 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.
5. Provider shall engage a sub-processor with respect to Processing of Accenture Personal Data that ensures at least the same level of data protection and security measures as agreed with Accenture. 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.
6. The Parties are responsible for maintaining a record of data subject requests and any other individual requests for information, the decisions made and any information that was exchanged. Records must include copies of the data subject request or other requests for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. The Party that collected the Personal Data directly from the data subject, shall be responsible for handling any data subject request coming from such data subject and, where appropriate, to provide the data subject with the requested information. The Parties shall provide reasonable assistance as is necessary to each other to enable them to comply with any data subject request and to respond to any other queries or complaints from data subjects.
7. 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 7 and will issue this certification to Accenture and/or Client upon reasonable request by Accenture/

SECTION II - PROVIDER'S ROLE – DATA PROCESSOR

To the extent that Provider Processes Personal Data as a Data Processor on behalf of Accenture and based on Accenture's instructions, the below terms shall apply and shall be considered as an integral part of the terms and conditions of the Agreement. Notwithstanding the above, if Provider is acting as a Data Controller of Accenture's Personal Data by determining the means and purposes of processing, Provider's Processing shall not be subject to this Data Privacy Schedule – Section II, but shall be in accordance with Section I.

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, including but not limited to, Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation ("**GDPR**").

"Information Security Obligations" means commercially reasonable and appropriate physical, technical and organisational security measures, including those set forth in the Agreement, along with its Schedules and Appendix 2 to the Standard Contractual Clauses (of Attachment A), which, at a minimum and when required, include for the purposes of the European Court of Justice judgment in Case C-311/18 (also known as "**Schrems II**") of 16 July 2020, measures which constitute supplementary measures.

"Personal Data" means any information relating to, identifying, describing or reasonably capable of being associated with or 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.

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, including Article 33 of the GDPR. 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 Provider Offerings 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 Provider Offerings relating to the Processing of Accenture Personal Data, or at 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 International Transfers of Personal Data.

Provider shall:

3.4.1 comply with the Standard Contractual Clauses Module 2 in Attachment A; and

3.4.2 ensure that the international transfer of Personal Data complies with Data Privacy Laws, and 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

3.4.3 provide, upon request by Accenture, reasonable assistance to Accenture and/or its clients with respect to any applicable filing, approval or requirements in relation to any agreement agreed under Data Privacy Laws.

Provider, acting as data importer, hereby explicitly acknowledges 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 in accordance with Data Privacy Laws. 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 the rights under Data Privacy Laws of the individuals to whom Accenture Personal Data relates are appropriately addressed without undue delay for the fulfilment of Accenture's obligation to respond to such requests under Data Privacy Laws, 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 (including Standard Contractual Clauses, Module 2 in Attachment A) 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 Articles 32 to 36 of the GDPR. If Accenture needs to provide information (including details of Provider Offerings) 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.

INFORMATION SECURITY SCHEDULE

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 Provider, as defined in the Agreement, and its third-party providers,suppliers,agents and subcontractors, and "**Accenture**" shall mean Accenture, as defined 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 Accenture 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 Offerings to Accenture and (ii) "**Provider Offerings**" shall mean the Technology and the Professional Offerings or have the meaning set forth in the Agreement including 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 Offerings.

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 (1) 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 Offerings 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 on Attachment 1 to 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 Offerings, deliverables, 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 all software components (including, but not limited to, open-source software) used in the Provider Offerings, 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 Offerings 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 Amazon Web Services 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 Offerings 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 Offerings, 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 Offerings 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. Infrastructure as a Service), vulnerability or security services as part of the Provider Offerings to Accenture or its Client, Provider agrees to undergo an assessment of such Provider Offerings and related deliverables and Provider will provide evidence that the agreed upon Provider Offerings are meeting the security requirements and/or specific Accenture Client requirements for the Provider Offerings (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 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 Statement on Standards for Attestation Engagements 18 ("SSAE18") Service Organization Control Type 2 ("SOC2 Type 2") report for identified locations and Provider Offerings, covering information security management implementation and operating effectiveness, that are used by Provider to develop software or deliver the Provider Offerings, 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 American Institute of Certified Public Accountants ("AICPA"), the International Auditing and Assurance Standards Board ("IAASB"), the Securities and Exchange Commission or the Public Company Accounting Oversight Board.

If Provider requests that Provider Offerings 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 Offerings being provided from such location.

Where the SSAE18 SOC2 Type 2 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, Service Organization Control Type 1 ("SOC 1") 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 eight (8) months of Accenture'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, the IAASB, the Securities and Exchange Commission or the Public Company Accounting Oversight Board.

Other than in connection with the provision of Provider Offerings pursuant to a Accenture-approved business continuity and / or disaster recovery assistance plan, if either Party requests that Provider Offerings, 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 Provider Offerings being provided from such location.

Accenture, at its own expense, may audit Provider (either at Provider's facilities or that portion of Provider's center from which Provider Offerings are provided to Accenture). Provider will permit Accenture, 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 Accenture requests a Accenture specific SSAE18 SOC1 report, Provider will contract with an internationally or nationally recognized independent public accounting firm to perform the Accenture specific audit. Accenture will be responsible for all costs associated with the Accenture specific audit. Accenture will be able to set the scope which shall be reasonably related to the Provider Offerings and those portions of the Provider locations from which Provider Offerings will be provided to Accenture, establish the control objectives, determine the frequency of such audit, and determine the reporting period.

ACCENTURE INFORMATION 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:

1. **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 Securit**y. 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.

2. **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 Offerings 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.

3. **Human Resource Security.**

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

4. 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 Offerings 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 Offerings 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 management (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."

5. 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 Offerings 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 Offerings 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 Offerings, 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 (Security Assertion Markup Language ("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 Offerings, 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 Provider web-based application(s) provided as part of the Provider's Offerings.

(vi) Provider shall maintain and enforce a password policy that is aligned to current Industry Standards (e.g., National Institute of Standards and Technology ("NIST") Cyber Security Framework, Payment Card Industry Data Security Standard ("PCI DSS"), Center for Internet Security) and default passwords must be changed before deploying any new asset. In the event that Provider Offerings includes the management of Accenture or its Client's infrastructure and environments, account lockout thresholds must be consistent with Accenture or its Client's account lockout standards, whichever is strictest.

(vii) Provider personnel, agents and contractors shall use multi-factor authentication and encrypted sessions for access to Provider systems. In the event that Provider Offerings require external connections to Accenture or Accenture Client's project dedicated environments, Accenture must provide approval of the connections.

6. 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.

7. Physical and Environmental Security.

a. Physical Access to Facilities. Provider shall limit access to facilities (where systems that are involved in providing the Provider Offerings 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 or 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.

8. 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, security and network devices that are involved in providing Provider Offerings. Logs must be kept for a minimum of six (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.

(i) 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.

(i) 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.

9. Communications Security.

a. Information Transfer and Storage.

(i) Provider shall use current Industry Standard encryption, Transport Layer Security ("TLS") minimum version 1.2, to encrypt Accenture Data that is in transit.

(ii) Provider shall use TLS, minimum version 1.2, over Simple Mail Transfer Protocol ("SMTP") 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 Offerings 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 Provider Offerings. 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 Offerings 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.

10. 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 SysAdmin, Audit, Network, and Security ("SANS") Top 25 Software Errors, the Open Web Application Security Project ("OWASP") Top 10 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 Offerings 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 Offerings 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 Offerings 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 Offerings 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 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 Offerings 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 Offerings prior to use and on a recurring basis no less frequently than once in a twelve (12)-month period by an industry recognized independent third party. 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.

11. 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.

12. 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, 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.

13. Compliance.

a. **Legal and Contractual Requirements**.

(i) Provisions regarding compliance with laws, intellectual property and data privacy are contained in the body of the Agreement and applicable schedules.

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.

Anti-corruption Schedule

In connection with the Provider Offerings performed pursuant to the Agreement, the Provider, which for purposes of this Schedule includes its owners, directors, officers, employees, representatives, partners, and agents:

1. Has not (other than to the extent disclosed to Accenture in writing in connection with this Anti-corruption Schedule) and will not violate the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act, or other applicable anti-corruption and anti-money laundering laws (collectively the "**Anti-corruption Laws**"), or otherwise offer or give money or anything of value to any person, in order to obtain or retain business for the benefit of Accenture or Provider, or to secure any other improper advantage for Accenture or Provider;
2. Will not submit any false or inaccurate invoices to Accenture or otherwise falsify any documents related to services performed for Accenture, and will submit true and adequate documentation with all invoices, including: a) an explanation of the services provided during the period covered by the invoice; and b) itemized expenses incurred, accompanied by receipts (or other documentation if a receipt is unavailable) identifying the payment date, amount and purpose of the expense;
3. Will not provide any gifts, meals, or entertainment to, or pay for the travel expenses of, any third party without the advance written approval of Accenture, and any such expenses shall comply with all applicable laws as well as the internal policies of the recipient's employer;
4. Will promptly notify Accenture in writing in the event that Provider fails to comply with the provisions of this Anti-corruption Schedule;
5. To the best of its knowledge has not, and will not enter into any actual or potential, interest in conflict with Accenture or with the services that would: (i) affect Provider's performance in the delivery of the services; (ii) affect any other aspect of the engagement letter; (iii) violate any law or regulation; or (iv) create any appearance of impropriety; and,
6. Agrees that in the event that Accenture has a good faith belief that there has been a breach of this Anti-corruption Schedule, Accenture may terminate its Agreement with Provider immediately upon written notice and without penalty. To report a serious concern, please call the Accenture Business Ethics Line at 0800-91-2270, available twenty-four(24) hours a day, seven(7) days a week (you can reverse the charges) or visit the encrypted website at https://businessethicsline.com/accenture.