ACCENTURE'S SERVICE PROVIDER STANDARDS OF COMPLIANCE AND ETHICS – France
(Revised November 2019)

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 / service 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 to Accenture as part of the Order:

- You adhere to the "standard code of conduct" https://www.accenture.com/_acnmedia/pdf-58/accenture-supplier-standards-of-conduct-final-en.pdf
- You declare to be in conformity with the warranties listed in the Certificate of Conformity (Schedule 1) on anti-corruption;

- You declare that you comply with the technical and operational requirements specific to security as defined in this document (Schedule 2);

- You declare to be in compliance with the personal data obligations defined in this document (Schedule 3).

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 SERVICE PROVIDER.

1 - DETERMINATION OF THE CONTRACTING PARTIES

Accenture, the Client, is understood to mean Accenture SAS, a ''société par actions simplifiée'' with a capital of 17,250,000 euros, with its registered office in Paris (75013) 118 avenue de France, registered with the ''RCS de Paris'' under number B 732 075 312 or any Accenture Group entity duly identified in the contractual document.

The Accenture Group is defined here as any company registered in France that is controlled within the meaning of Article L233-3 of the French Commercial Code by Accenture Holdings France SAS, a ''société par actions simplifiée'' with a capital of 407,037,000.00, euros whose head office is in Paris (75013) 118 avenue de France, RCS PARIS 477 832 612.

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

2 – DOCUMENTS TO BE PROVIDED BY THE SERVICE PROVIDER/ SUPPLIER REGARDING THE LAWS ON ILLEGAL WORK

Please consider with attention the following note reminding your legal and contractual obligations toward Accenture. Accenture reminds you that your failure to comply with these legal obligations entitles Accenture to terminate the contractual relationship (Agreement) immediately by written notice and without penalty.

Accenture designated PROVIGIS as collector of the following documents. Please fill in your supplier profile on: http://www.provigis.com

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

All documents must be written in French and provided every six months until the end of the Agreement.

Service provider / supplier established or residing 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 6 months old.
2. A copy of the excerpt from the registration in the Register of Commerce and Companies (KBIS).
3. The certificate of professional insurance.
4. In the case of foreign employees, subject to a work authorization (Article D8254-2 of the Labour Code): a list of names specifying, for each employee, the date of recruitment, the nationality and the type and serial number of the employee. title is a work permit ("Nominative List of Foreign Workers").

Service provider / supplier / contractor / consultant 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)
http://travail-emploi.gouv.fr/IMG/pdf/IT_300-2.pdf
Copy of the mandate of representation of the supplier in France (Cerfa 13816-02)
For complementary informations:
http://travail-emploi.gouv.fr/europe-et-international/detachement-des-salaries/article/temporary-posting-of-workers-in-france
and the guide created to the attention of foreign service providers:
http://travail-emploi.gouv.fr/IMG/pdf/Guide_employeur_en_Anglais.pdf

3- COMPLIANCE WITH LAWS

Each Party covenants to comply with all applicable laws, ordinances and regulations, including the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, and all other applicable anti-corruption laws, anti-competition laws, and export compliance laws. The Service Provider will not 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.

Service Provider agrees to execute all the warranties, declarations and commitments defined in the ''Certification of Acknowledgement and Compliance'', a copy of which is attached hereto as Schedule 1 (the "Certification of Acknowledgement and Compliance").

Records and Audit Rights: Throughout the duration of the commercial relations with Accenture and for thirty-six (36) months thereafter, The Service Provider will retain and, upon reasonable notice, will provide Accenture reasonable access to audit its books, accounts, and records relating to the Services performed and payments made by the Service Provider in connection with performance of the Services. At the Service 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/non-disclosure agreement. The Service Provider shall cooperate fully in any audit conducted by or on behalf of Accenture or of its Clients.

IF YOU DO NOT EXTEND THE WARRANTIES, DECLARATIONS AND COMMITMENTS OF THE CERTIFICATE, 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).

4 – 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 Schedule 2 "Information Security" 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 (IDENTIFIED IN THE PO).

5 – PERSONAL DATA

The Service Provider and Accenture undertake to comply with the provisions of the French law "Informatique et Libertés" n ° 78-17 of 6 January 1978 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 Service 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 Schedule 3.

The Service Provider is advised that Accenture implements a processing of personal data to manage its relations with its own service 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 service 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 Service Provider's employees may be exercised by mail to the Procurement contact person 118 avenue de France 75013 Paris, accompanied by a copy of an identity document or by e-mail to the Accenture Data Privacy Officer at dataprivacy@accenture.com. It is the responsibility of the Provider to inform its employees of this clause.

SCHEDULE 1: CERTIFICATION OF ACKNOWLEDGEMENT AND COMPLIANCE

The Service Provider which for purposes of this Certification 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 Certification) 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 Anticorruption 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 Business Intermediary, or to secure any other improper advantage for Accenture or Business Intermediary;

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 and without delay in the event that the Service Provider fails to comply with the provisions of this Certification;

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 Service 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;

6. Agrees that in the event that Accenture has a good faith belief that there has been a breach of this Certification, Accenture may terminate its Agreement with Service Provider immediately upon written notice and without penalty. 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;

7. In case Service Provider has to implement a compliance program regarding anticorruption in application of the Law n°2016-1691 « loi Sapin II », the Service Provider certifies the good implementation of the program and provides Accenture with the relevant evidences and certificates at first request.

SCHEDULE 2: INFORMATION SECURITY REQUIREMENTS

1. INFORMATION SECURITY REQUIREMENTS

1.1 Where Service Provider knows, or reasonably suspects, that a loss, unauthorized acquisition, disclosure, use or other form of compromise of Accenture Data has occurred, Service Provider will notify Accenture's point of contact in writing promptly, and in any event within forty-eight (48) hours following such discovery and cooperate with Accenture in any breach investigation or remediation efforts. For the purposes of this Information Security Schedule: (i) "**Accenture Data**" shall 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 Service Provider in connection with providing the applicable Services to Accenture, including Accenture Personal Data as defined in the Agreement; and (ii) "**Services**" shall have the meaning set forth in the Agreement and also includes any other services provided by the Service Provider under the Agreement, and shall include any software and equipment provided by Service Provider (including third party software and equipment) required to access the Services or provide the Services.

1.2 Service Provider represents and warrants that it shall implement appropriate technical and organizational security measures, based on Industry Standards. "Industry Standards" means commercially reasonable security measures in all applicable equipment, software systems and platforms that Service 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 the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Accenture Data, including those safeguards, practices and procedures prescribed in at least one of the following:

i. ISO / IEC 27000-series – see http://www.iso27001security.com/; 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. 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
v. When "Protected Health Information" is stored, accessed, viewed, or processed: Health Insurance and Portability Accountability Act ("**HIPAA**"): http://www.hhs.gov/hipaa/.

Further, Service 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 by Accenture in its business operations. Upon Accenture's request, Accenture Data shall be immediately returned to Accenture by Service Provider, either, at Accenture's option, using the Services or in an Industry Standard format specified by Accenture.

Service 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, procedures 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 Service Provider.

1.3 Illicit Code. Except for the functions and features expressly disclosed in Service Provider's documentation provided or made available to Accenture, at the time of delivery or transmission to Accenture, an Accenture Affiliate, or a Client of any Services, software, equipment, or deliverables, or at the time Service Provider makes such items available to Accenture, an Accenture Affiliate or a Client, as applicable, such Services, software, equipment and/or deliverable shall be free of any programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, malware, worms, date bombs, time bombs, shut-down devices, keys, authorization codes, back doors or passwords allowing Service Provider access), that may result in, either: (a) any inoperability of the Services, software, equipment, or deliverable; or (b) any damage, interruption, interference with the operation of the Services, software, equipment, or deliverable, the equipment configuration on which the Services, software, or deliverables reside, any other software or data on such equipment configuration, or any other equipment or system with which the equipment configuration, Services, software or deliverable is capable of communicating.

1.4 Security of All Software Components. Service Provider agrees to appropriately inventory all software components (including, but not limited to, open source software) used in Service Provider's Services, software, equipment and/or deliverables, and provide such inventory to Accenture upon request. Service Provider will assess whether any such software components have any security defects and / or vulnerabilities that could lead to unauthorized disclosure of Accenture Data or intellectual property of Accenture or its clients. Service Provider shall perform such assessment 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. Service Provider agrees to notify Accenture of any identified security defect or vulnerability and remediate same in a timely manner. Service Provider will promptly notify Accenture of its remediation plan. If such security defect or vulnerability cannot be remediated in a timely manner, Service Provider agrees to replace the subject software component with a component that is not affected by this security defect or vulnerability and that does not reduce the overall functionality of the Services, software, equipment or deliverables being provided under this Agreement. Service 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 Disaster Recovery. During the term of the Agreement and all Orders, Service Provider shall maintain a disaster recovery (DR) or highly availability (HA) solution and related plan that is consistent with Industry Standards for the 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) so that if one tier and/or one physical data center were affected, the application would continue to run uninterrupted on the nodes in the unaffected location.
- The DR solution will ensure identified critical capabilities are restored within a 24-hour period in the event of a declared disaster or major system outage. A DR plan will ensure critical capabilities automatically fail over or can be manually failed over within a 60-minute period in the event of a declared disaster or major system outage affecting a location.

Service Provider will test the DR or HA solution and related plan at least once every six (6) months or more frequently if test results indicate that critical systems were not capable of being recovered within the periods above. Service 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 Services, if not automated failover) achieved within the exercise. Service 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 from being recovered within 24 hours in the event of a disaster or major system outage.

2. SECURITY ASSESSMENT

2.1 Security Assessment. In the event that Accenture reasonably determines, or in good faith believes, that Service Provider's security practices and procedures do not meet Service Provider's obligations pursuant to the Agreement or this Information Security Schedule (including Attachment 1 hereto), then Accenture will notify Service Provider of the deficiencies. Further, Service 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 Service Provider's and Service Provider agents' security-related activities that are relevant to the Agreement. Additionally; Service Provider will complete, in a timely and accurate manner, an information security questionnaire, provided by Accenture to Service Provider, on an annual basis or more frequently upon Accenture's request, in order to verify Service Provider's and its sub-contractors' compliance with the Agreement. ("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 agreed to timeframe to remediate. Service Provider shall remediate all of the security issues identified within the agreed to remediation timeframes. If Service Provider fails to remediate any of the high or medium rated security issues within the stated remediation timeframes, Accenture reserves the right to terminate this Agreement for material breach immediately upon notice to Service Provider.

3. CONTROL AUDIT RIGHTS

SSAE18 SOC2 Reports

During each calendar year, Service Provider will provide, at Service Provider's cost, a SSAE18 SOC2 Type II reports for identified locations that are used by Service Provider to develop software or deliver the 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. The coverage period of such reviews will cover at least eight 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 Service Provider and Accenture. Service 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 Service Provider requests that 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 Services being provided from such location.
In addition to the SSAE18 SOC 2 report provided above, Accenture, at its own expense, may further audit Service Provider (either at Service Provider's facilities or that portion of Service Provider's facilities from which Services are provided to Accenture or in which the software is developed). Service Provider will permit Accenture, or its duly authorized representatives, on reasonable prior notice, to assess Service Provider's and its Service Provider agents' activities that are relevant to this section. If Accenture requests an Accenture specific SSAE18 SOC 2 report, Service Provider will contract with an internationally 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 set the scope of the report (which shall be reasonably related to the Services or software development and those portions of the Service Provider locations from which Services will be provided to Accenture or in which the software is developed), establish the controls to achieve the criteria, determine the frequency of such audit, and determine the reporting period.

ATTACHMENT 1 TO SCHEDULE 2 - SECURITY REQUIREMENTS

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

1. Information Security Policies

a. **Policies for Information Security**. Service Provider's policies for information security shall be documented by Service Provider, approved by Service Provider's management, published and communicated to Service Provider's personnel, contractors, agents and relevant external third-parties.
b. **Review of the Policies for Information Security**. Policies for information security shall be reviewed by Service Provider at least annually, or promptly after material changes to the policies occur, to confirm applicability and effectiveness. Service Provider shall not make changes to the policies that would materially degrade security obligations without first providing notice to Accenture.

2. Organization of Information Security

a. **Security Accountability**. Service Provider shall assign one or more security officers who will be responsible for coordinating and monitoring Service Provider's information security function, policies, and procedures.
b. **Security Roles and Responsibility**. Service Provider personnel, contractors and agents who are involved in providing Services shall be subject to confidentiality agreements with Service Provider.
c. **Risk Management**. Appropriate information security risk assessments shall be performed by Service 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. Upon request, Service Provider will meet with Accenture at least annually to discuss information security related to the Services and shall provide summary reports of applicable risk assessments to Accenture.

3. Human Resource Security

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

4. Asset Management

a. Asset Inventory. Service 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 Service Provider.

b. Asset Handling

i. Service Provider shall classify Accenture Data so that it is properly identified and access to Accenture Data shall be appropriately restricted.
ii. Service 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 Services under the Agreement.
iii. Service 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 Service Provider facilities. If remote access is approved and granted, Service Provider personnel, agents and contractors shall use multi-factor authentication. Multi-factor authentication may include techniques such as the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.

5. Access Control.

Service Provider shall maintain an appropriate access control policy that is designed to restrict access to Accenture Data and Service Provider assets to authorized personnel, agents and contractors.

a. Authorization

i. Service 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 Services under the Agreement. The Service Provider will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.
ii. Service Provider shall maintain and update records of personnel who are authorized to access Service Provider systems that are involved in providing Services and review such records at least quarterly.
iii. Service Provider shall ensure the uniqueness of user accounts and passwords for each individual. Individual user accounts must not be shared.
iv. Service Provider shall remove access rights to assets that store Accenture Data for personnel and contractors 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. Service Provider will perform periodic access reviews for system users at least quarterly for all supporting systems requiring access control.

b. Least Privilege Access

i. Service Provider shall restrict access to Service Provider systems involved in providing 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.

c. Authentication

i. Service Provider will use Industry Standard capabilities to identify and authenticate personnel, agents and contractors who attempt to access information systems and assets.
ii. Service Provider shall maintain Industry Standard practices to deactivate passwords that have been corrupted or disclosed.
iii. Service Provider shall monitor for repeated access attempts to information systems and assets.
iv. Service Provider shall maintain 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. Service Provider shall provide an Industry Standards based single sign-on (SSO) capability (SAML, etc.) for Accenture which will require authentication to access any Service Provider web-based application(s) provided as part of the 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 waived, multi-factor authentication is still required for access to Service Provider web-based application(s) provided as part of the Services.
vi. Service Provider will require that all accounts have complex passwords that contain letters, numbers, and special characters, be changed at least every 90 days, and have a minimum length of 8 characters.
vii. Service Provider shall use multi-factor authentication for all administrative access, including domain and cloud portal administrative access. Multi-factor authentication may include techniques such as the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.

6. Cryptography.

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

7. Physical and Environmental Security

a. Physical Access to Facilities. Service Provider shall limit access to facilities (where systems that are involved in providing the Services are located) to identified personnel, agents and contractors.

b. Physical Access to Components. Service 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.

c. Protection from Disruptions. The Service 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. Service 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. Service Provider shall adopt a clear desk policy for papers and removable storage media and a clear screen policy.

8. Operations Security

a. Operations Policy. Service 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. Service Provider must enable logging and monitoring on all operating systems, databases, applications, security and network devices that are involved in providing 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. Service Provider shall maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks. Service Provider shall maintain software at the then current major release for Service Provider owned anti-malware software and provide maintenance and support for new releases and versions of such software.

d. Backup. Service Provider shall maintain a 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 Service Provider policy unless other such Accenture requirements are agreed upon. Service Provider shall regularly test restoration procedures.

e. Vulnerability Management. Service Provider shall have policies that govern the installation of software and utilities by personnel.

f. Change Management. Service Provider shall maintain and implement procedures to ensure that only approved and secure versions of the code / configurations / systems / applications will be deployed in the production environment(s).

g. Encryption of Data at Rest. Service Provider shall encrypt data at rest using a commercially supported encryption solution or shall provide the capability with instructions to Accenture so that Accenture may enable further encryption, at Accenture's discretion. Encryption solutions will be deployed with no less than 256-bit Advanced Encryption Standard (AES) encryption.

9. Communications Security

a. Information Transfer.

i. Service Provider shall use Industry Standard encryption to encrypt Accenture Data that is in transit.

ii. Service Provider shall restrict access through encryption to Accenture Data stored on media that is physically transported from Service Provider facilities.

b. Security of Network Services. Service 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.

c. Intrusion Detection. Service Provider shall deploy intrusion detection or 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. Service 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.

10. System Acquisition, Development and Maintenance

a. Workstation Encryption. Service Provider will require hard disk encryption of at least 256 bit Advanced Encryption Standard (AES) 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 Service Provider will maintain and implement secure application development policies, procedures, and standards that are aligned to Industry Standard practices such as the SANS Top 35 Security Development Techniques and Common Security Errors in Programming and the OWASP Top Ten project. 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 Services and receive appropriate training regarding Service Provider's secure application development practices.

c. System Hardening.

i. Service Provider will establish and ensure the use of standard secure configurations of operating systems. Images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening includes: removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and use of host-based firewalls. These images should be validated on a regular basis to update their security configuration as appropriate.

ii. Service Provider will perform periodic access reviews for system administrators at least quarterly for all supporting systems requiring access control.

iii. Service Provider will implement patching tools and processes for both applications and for operating system software. When outdated systems can no longer be patched, Service Provider will update to the latest version of application software. If this is not possible, Service Provider shall notify the Accenture so that an appropriate risk assessment can be conducted. Service Provider will remove outdated, older, and unused software from the system.

iv. Service 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. Service Provider shall scan its internal environment (e.g. servers, network devices, etc.) related to Services on a monthly basis and external environment related to Services on a weekly basis. Service Provider shall have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days.

e. Application Vulnerability Assessment. Service Provider will perform an application security vulnerability assessment at least once per year. The test must cover all web application vulnerabilities defined by the Open Web Application Security Project (OWASP) or those listed in the SANS Top Cyber Security Risks or its successor current at the time of the test. Service Provider will provide a summary of the vulnerability assessment results upon request.

f. Penetration Tests and Security Evaluations of Websites. Penetration Tests and Security Evaluations of Websites. Service Provider shall perform a comprehensive penetration test and security evaluation of all systems and websites involved in providing Services prior to use and on a recurring basis no less frequent than once every three months. Additionally, Service Provider will have an industry recognized independent third party perform one of the quarterly tests. Service Provider shall have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days. Service Provider shall provide a summary of the penetration test and

security evaluation, including any open remediation points, to Accenture upon request.

11. Service Provider Relationships

a. Where other third-party applications or services must be engaged by Service Provider, Service Provider's contract with any third-party must clearly state security requirements consistent with the security requirements of this Information Security Schedule which will be applied to the third party. 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. Service Provider shall conduct security reviews of third-party suppliers to address physical and logical security requirements, privacy protection, breach reporting, and contractual requirements..
d. Service Provider will perform quality control and security management oversight of outsourced software development.

12. Information Security Incident Management

a. Incident Response Process

i. A "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to any Accenture Data stored on Service Provider's equipment or in Service Provider's facilities, or unauthorized access to such equipment or facilities resulting in the loss, disclosure, or alteration of Accenture Data.

ii. Service 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.

iii. In the event of a Security Incident, Service Provider will: (a) notify Accenture of the Security Incident by contacting their Accenture point of contact in writing promptly, and in any event within forty-eight (48) hours, following the discovery of the Security Incident; (b) promptly investigate the Security Incident; (c) promptly provide Accenture with all relevant detailed information about the Security Incident; and (d) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

iv. The Service 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.

SCHEDULE 3 –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. Service 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).

"**Business Contact Information**" means any Personal Data that is used for the purpose of communicating, or facilitating communication, with an individual in relation to their employment, business or profession, such as their name, position name/title, work address, work phone number, work fax number or work e-mail.

"**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").

"**Personal Data**" means any information relating to an identified or identifiable natural person (or, to the extent that applicable Data Privacy Laws apply to information about legal persons, an identified or identifiable legal person) or as otherwise defined in 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.

2. NO SERVICE PROVIDER ACCESS TO ACCENTURE PERSONAL DATA

2.1 Except as provided in Section 3, Service Provider shall not access, nor seek access to (including seeking to acquire the means to access), Accenture Personal Data. Service Provider shall contractually obligate its sub-contractors and/or sub-processors to comply with this obligation.

2.2 If Service Provider (or any of its sub-contractors and/or sub-processors) accesses, or has access to, or acquires the means to access, Accenture Personal Data, then Service Provider shall (and shall ensure that any relevant sub-processor and/or sub-contractor):

2.2.1 promptly notify Accenture that this is the case; and

2.2.2 avoid further accessing or Processing, or seeking to further access or Process, such Accenture Personal Data; and

2.2.3 promptly and securely return all such Accenture Personal Data to Accenture.

2.3 Service Provider shall not engage a sub-processor without Accenture´s prior written approval, in which case the Service Provider and applicable sub-processor(s) must be bound by a written agreement that includes the same data protection obligations on the sub-processor(s) as agreed between Service Provider and Accenture. Service Provider will remain fully liable to Accenture for any act or omission of the sub-processor in the performance of that sub-processor´s obligations.

3. BUSINESS RELATIONSHIP DATA

Either Party may receive Business Contact Information of the other Party, as part of maintaining its business relationship under the Agreement. Service Provider will Process Accenture's Business Contact Information in accordance with Data Privacy Laws. Personal Data may also be obtained by Accenture indirectly through internal security systems or other means. Accenture will Process Service Provider's 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 Service Provider upon request). For such purposes, Accenture may transfer the applicable Personal Data to any country where Accenture's global organization, its clients and its Service Providers operate. If required by Data Privacy Laws, Accenture and Service Provider agree to sign any additional agreement or amendment that may be required to allow the transfer of such Personal Data outside its jurisdiction of origin.

4. CHANGES IN DATA PRIVACY LAWS

In the event of any changes in Data Privacy Laws applicable to Accenture Personal Data, that result in new requirements (including new physical, technical, organizational, security, or data privacy measures), Service Provider will reasonably cooperate with Accenture in designing a remedial response to implement such new requirements.