

# G-Cloud 10 Terms & Conditions



## Accenture Terms & Conditions

May 2018

Contents

Master Services Agreement (“MSA”) .....4

Schedule 1 .....10

Exhibit A (Statement of Work).....12

Exhibit B (Certus Support Services).....15

Exhibit C (General Accenture Cloud Service Terms and Conditions) .....25

Appendix A – Definitions .....34

Service Order.....35

Attachment A Security Standards .....37

Attachment B Encryption and Security Architecture Requirements .....38

Service Order.....39

Service Order.....41

Attachment A: Service Levels .....42

**[Due to constraints in uploading multiple documents, we have consolidated the terms and conditions for our services into this single document. The Master Services Agreement and Exhibit A (Statement of Work) are intended to apply to all services. Where applicable, Exhibit B (Certus Support Services) and/or Exhibit C (General Accenture Cloud Service Terms and Conditions) with a relevant Service Order may also apply.]**

# Master Services Agreement (“MSA”)

1. **Services.** Accenture (UK) Limited whose registered office is located at 30 Fenchurch Street, London EC3M 3BD (“Accenture”) will provide the services (“Services”) and deliverables (“Deliverables”) to [xxx] whose registered office is located at [xxx] (“Client”) as specified in separately signed Statements of Work (SOWs), under the following terms and conditions (collectively the “Agreement”):
2. **Confidentiality.**
  - 2.1 Each party may have access to information (in any form) that relates to the other party’s past, present, and future activities including research, development, business activities, products, services, processes and technical knowledge, which is identified by the disclosing party as confidential or reasonably understood to be confidential (“Information”).
  - 2.2 Information may only be used by the receiving party consistent with the rights and obligations of this Agreement. The receiving party agrees to protect the Information of the disclosing party in the same manner that it protects its own similar confidential information, but in no event using less than a reasonable standard of care. Access to the Information will be restricted to Accenture and Client personnel (including such personnel employed by their affiliates) and subcontractors pursuant to the parties’ rights and obligations under this Agreement, provided such parties are bound by substantially similar obligations of confidentiality. Accenture may retain and use Information relevant to its business purposes (including to provide or enhance our services) so long as its use of such Information is in an aggregated and anonymised or pseudonymised manner. Information that identifies or directly relates to natural persons (“Personal Data”) is treated separately from other Information.
  - 2.3 Nothing in this Agreement will prohibit or limit either party’s use of information (i) previously known to it without an obligation not to disclose such information, (ii) independently developed by or for it without use of the information, (iii) acquired by it from a third party which was not, to the receiver’s knowledge, under an obligation not to disclose such information, or (iv) which is or becomes publicly available through no breach of this Agreement.
3. **Data Protection and Personal Data.** Accenture has complied and will continue to comply with its obligations as data processor arising from the data protection and privacy laws in force from time to time to the extent that those obligations are relevant to this Agreement. Client will likewise comply with its obligations as data controller. Each party will exercise commercially reasonable efforts not to disclose any Personal Data to the other party and to restrict the other party’s access to its Personal Data. If a party is given access to the other party’s Personal Data (other than in connection with the Services), the receiving party will protect such Personal Data as required by applicable data protection and privacy laws, including implementing and maintaining an information security program with reasonable administrative, technical, organisational and physical measures designed to secure and protect the confidentiality, integrity and availability of all Personal Data while in such party’s possession against unauthorised, unlawful or accidental access, disclosure, transfer, destruction, loss or alteration. If Accenture requires access to Client’s Personal Data in connection with the Services for a particular project under this Agreement, the parties will agree in the applicable SOW on the procedures and obligations of each party with respect to the access, use and protection of such Personal Data and where needed implement additional data security controls and processes for the transmission, transfer outside the EEA, exchange, storage, processing or other use of Personal Data as described in such procedures.
4. **Acceptance.** All Services and Deliverables will be deemed accepted if not rejected by Client by providing written notice within ten (10) business days after delivery specifically identifying the manner in which the Services or Deliverables fail to materially comply with their applicable specifications. Deliverables will be those items created for Client by Accenture which are specified in an SOW.
5. **Intellectual Property.**
  - 5.1 All software, patents, graphics, photos, designs, trademarks, logos or other artwork and materials provided to Accenture by Client under this Agreement (“Client IP”) are and shall remain the sole and exclusive property of Client or its third party licensors and Client shall obtain any relevant consents and licences necessary for Accenture to use Client IP to perform Services and provide Deliverables under this Agreement. Client hereby grants to Accenture, during the term of this Agreement, a non-exclusive, fully paid, worldwide, non-transferable, limited licence to use and permit Accenture’s subcontractors to use the Client IP, solely for the purposes of providing the Services and Deliverables under this Agreement.
  - 5.2 Effective upon final payment, Accenture hereby grants to Client, subject to any restrictions applicable to any third party materials embodied in the Deliverables, a perpetual, worldwide, nontransferable, non-exclusive, irrevocable right and licence to use, copy, modify and prepare derivative works of the Deliverables for purposes of Client’s and its affiliated companies’ internal business only (excluding any Accenture IP, defined below, governed by separate licence agreements signed by Client (if any)). All intellectual property in the Deliverables remain in and/or

are assigned to Accenture. All other intellectual property: (a) of Accenture existing prior to the Services, (b) used in the Services (except Client IP), (c) developed by Accenture, or (d) licensed to Accenture by third parties and used in the Services, and (e) any enhancements or modifications to, or derivative works of, any intellectual property in categories (a) to (d), are the sole and exclusive property of Accenture ("Accenture IP"). Accenture IP embedded in Deliverables may not be used separately or beyond the licence rights granted above. The Deliverables and Accenture IP are proprietary to Accenture and embody valuable intellectual property rights, which may include Accenture patents, copyrights, trade secrets, know-how and other proprietary rights. Client agrees to pay a licence fee, if any, specified in the applicable SOW for the rights granted herein.

- 5.3 Each party is otherwise free to use concepts, techniques and know-how retained in the unaided memories of those involved in the performance or receipt of the Services. Accenture is not precluded from independently developing for itself, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the Deliverables provided and to the extent that they do not contain Client Information.
- 5.4 Within ten (10) business days of termination of this Agreement for any reason, Accenture will destroy or return any Client IP in Accenture's possession to Client (subject to retaining copies of any information required for its internal recordkeeping requirements). Third-party intellectual property, such as the licensing of third-party assets or third-party components, may require additional terms of usage, which will be addressed in an SOW where applicable.
6. **Payment and Taxes.** Accenture will, at the beginning of each month, invoice Client for the fees for that month, plus any applicable out-of-pocket expenses and applicable taxes; any necessary adjustments to the actual fees or expenses incurred will be made in the next month's invoice. Billable expenses will be billed at actuals. All invoices submitted to Client for payment will be itemised in reasonable detail. Payment for undisputed amounts is due by electronic transfer within thirty (30) days of Client's receipt of each invoice. Should any invoice (excluding disputed amounts) remain unpaid for more than thirty (30) days, interest will be paid at a rate of 1% per month or the highest rate allowed by law, whichever is less. Each party will be responsible for its own income, employment and property taxes. The parties will cooperate in good faith to minimise taxes to the extent legally permissible and will provide to the other any tax exemptions or certification reasonably requested. Client will be responsible for payment of all taxes in connection with this Agreement including withholding taxes and taxes incurred on transactions between and among Accenture, its Affiliates, and third party subcontractors. Client will reimburse Accenture for any deficiency relating to taxes that are Client's responsibility under this Agreement. If work for Client requires that personnel perform Services outside the city, state, province, or country in which such personnel are based, Client will reimburse Accenture for increased tax and administrative costs incurred by Accenture and/or its personnel. SOWs may further specify varied or other payment structures.
7. **Warranties.** Accenture warrants that its Services will be performed with reasonable skill and care, in accordance with this Agreement. In addition, each party warrants that upon its execution, this Agreement will not materially violate any term or condition of any agreement that such party has with any third party and that the officer(s) executing this Agreement are authorised to bind such party to the terms and conditions hereof. Accenture will re-perform any work not materially in compliance with this warranty brought to its attention within thirty (30) days after that work is performed. The preceding are the only warranties concerning the services, any deliverables or materials, or this Agreement, and (to the extent permitted by law) are made expressly in lieu of all other warranties, conditions, terms, representations and/or undertakings, express or implied, statutory or otherwise, including (without limitation) as to condition, performance, fitness for purpose, satisfactory quality, informational content, systems integration, non-infringement, interference with enjoyment, or otherwise.
8. **Indemnities.**
- 8.1 Each party (the "Indemnifying Party") will indemnify, save, and defend the other party, its parents, subsidiaries, affiliates, successors, and their directors, officers, employees, agents and representatives (collectively the "Indemnified Parties"), from and against any and all third party claims, demands, lawsuits, judgments, fines and penalties (including interest thereon and court costs) caused by a claim that any Deliverable (in which case Accenture is the Indemnifying Party) or Client IP (in which case Client is the Indemnifying Party) provided pursuant to this Agreement (collectively, "Indemnified Claims") (i) infringes a third party's copyright, trademark, or UK patent existing as of the date of delivery of such Deliverable or Client IP, or (ii) misappropriates a third-party's trade secrets;
- 8.2 The Indemnifying Party will have no liability to any Indemnified Party to the extent that the alleged infringement or misappropriation was caused by: (i) modifications to any Deliverable (made by or on behalf of Client) or Client IP (made by or on behalf of Accenture); (ii) use of the Deliverable or Client IP in combination with any hardware, software or other products or services where such combination was not within the reasonable contemplation of the Parties; (iii) the failure of an Indemnified Party to use corrections or enhancements to the Deliverable or Client IP provided by the Indemnifying Party; (iv) specifications or direction provided by the Indemnified Party; or (v) use

of the Deliverable or Client IP not authorised under this Agreement. If any Deliverable is, or in Accenture's opinion is likely to be, held to be infringing, Accenture will at its expense and option either: (i) procure the right for Client to continue using it, (ii) replace it with a non-infringing equivalent, (iii) modify it to make it non-infringing, or (iv) direct the return of the Deliverable and refund to Client the fees paid for such Deliverable. This section sets forth the sole and exclusive remedies for Indemnified Claims. To receive the benefits of this provision, the Indemnified Party must promptly notify the Indemnifying Party in writing of any eligible claim or demand and provide the Indemnifying Party reasonable cooperation and full authority to defend or settle the same provided that such settlement does not impose any obligation (monetary or otherwise) on the Indemnified Party without its consent.

9. **Liability.** Except for each party's obligation of indemnification set forth above, the sole liability of either party to the other for any and all claims in any manner related to this Agreement (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) will be for direct damages, not to exceed (in the aggregate) an amount equal to the total fees paid or payable to Accenture under the applicable SOW (or, if the term of the SOW is 24 months or longer, the amount of the aggregate cap shall be limited to the fees paid or payable during the 12 month period immediately preceding the event giving rise to the first such claim). In no event will either party be liable for any: (a) consequential, indirect, or punitive damages; or (b) business interruption, lost business, lost profits or goodwill or reputation or lost savings (anticipated or otherwise) (in each case whether direct or indirect), or (c) losses or claims arising out of or related to Client's implementation of any Deliverables or recommendations provided by Accenture. Nothing in this Agreement excludes or limits either party's liability to the other which cannot lawfully be excluded or limited including, without limitation, liability for death or personal injury caused by negligence or fraud.
10. **Compliance with Laws.** Each party will retain responsibility for compliance with all laws and regulations applicable to their respective businesses. Each party shall retain responsibility for its compliance with all applicable export control laws and economic sanctions programs relating to its respective business, facilities, and provision of services to third parties. Accenture shall not be required by the terms of the Agreement to be directly or indirectly involved in the provision of goods, software, services and/or technical data that may be prohibited by applicable export control or economic sanctions programs if performed by Accenture. Prior to providing Accenture any goods, software or technical data subject to export controls, Client will provide written notice to Accenture specifying the nature of the controls and any relevant export control classification numbers.
11. **Termination.** In addition to any termination rights of the parties in an SOW, either party may, upon giving thirty (30) days written notice identifying specifically the basis for such notice, terminate for material breach of this Agreement unless the party receiving the notice cures such breach within the thirty (30) day period. In the event this Agreement is terminated, Client will pay Accenture for all Services rendered and expenses incurred prior to the date of termination according to the monthly billing cycle set forth in the Agreement and any out of pocket demobilisation costs if Accenture terminates this Agreement for cause. All provisions of this Agreement which are by their nature intended to survive the expiration or termination of this Agreement will survive such expiration or termination. Termination of the Agreement does not affect the remaining term of any SOW.
12. **Disputes.** The parties will make good faith efforts to first resolve internally any dispute, including over an invoice, in connection with this Agreement. The party raising any dispute shall first serve written notification to the other party. Within thirty (30) days of the service of such notice one director or other senior representative of each party with authority to settle the dispute shall meet to seek to resolve the dispute. If within thirty (30) days of service of the notice no meeting has taken place or the dispute has not been resolved, either party shall be entitled to refer the dispute to the courts in accordance with this clause. In the event that Client shall hold an amount equal or greater to two months' average fees under any SOW, then Accenture will be permitted to suspend performance until such time as the matter in dispute is resolved. This Agreement shall be governed by and construed in accordance with the laws of England, without regard to its conflict of laws provisions and each party irrevocably submits to the jurisdiction of the courts of England in respect of any litigation in connection with this Agreement.
13. **Relationship.** Each party is an independent contractor and does not have any authority to bind or commit the other. Nothing in this Agreement will be deemed or construed to create a joint venture, partnership, fiduciary or agency relationship between such parties for any purpose. Neither party will solicit, offer work to, employ, or contract with, directly or indirectly, any of the other party's Personnel during their participation in the Services or during the twelve (12) months after the conclusion of such Services. "Personnel" means any individual or company a party employs or has employed as a partner, employee or independent contractor and with which a party comes into direct contact in the course of the Services. However, this section will not apply to Personnel who independently respond to indirect solicitations (such as general newspaper advertisements, employment agency referrals and internet postings) not targeting such Personnel. If Accenture subcontracts any Services under this Agreement, it is understood that Accenture is responsible for its subcontractors' performance. In this Agreement, "affiliate" of a party means another entity that, directly or indirectly, through one or more

intermediaries, is controlled by or under common control of that party, and control means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of the party, whether through share ownership, holding of voting power, contract or otherwise.

14. **Relief.**

14.1 In addition to any other Client responsibilities or assumptions described in any SOW, set forth below at Section 14.2 is a non-exhaustive list of the obligations for which Client will be responsible, conditions on Accenture's performance, and assumptions upon which Accenture relies in agreeing to perform the Services described under the Agreement and any applicable SOW on the terms set out herein (collectively "**Client Obligations**"). If any of the Client Obligations are not performed or prove to be incorrect (a "**Relief Event**"), it may cause changes to the project schedule, fees and expenses, Deliverables, level of effort required, or otherwise impact Accenture's performance of the Services to be carried out under this Agreement and any applicable SOW. In the event of a Relief Event, Accenture shall have no liability with respect to its inability to perform the Services resulting therefrom. Client shall grant to Accenture such additional time as is reasonable to provide the Services and/or the relevant Deliverables, as the case may be, and shall pay to Accenture any additional fees necessary to compensate Accenture for any necessary additional effort or expenses.

14.2 The Client Obligations shall include (but shall not be limited to): (i) the Client shall set overall direction for the project team, make choices on direction, options and priorities, and take ownership for the outcomes; (ii) the Client will commit the necessary resources and management involvement to support the project and perform the agreed upon acceptance procedures in Section 4 in a timely manner, and who have access to tools and data required for the project; (iii) decisions to be made by the Client will be made promptly and without delay; (iv) client shall be responsible for obtaining, at no cost to Accenture, consents for Accenture's use of any third party products, including, but not limited to software (including purchase of any licences), necessary for Accenture to perform its obligations under this Agreement and any applicable SOW; (v) Client shall be responsible for the performance of other contractors or vendors engaged by Client in connection with the project and ensuring that they cooperate with Accenture; (vi) any Confidential Information disclosed to third parties contracted by the Client shall be subject to the confidentiality obligations of the Agreement; (vii) the Client shall be responsible for its operation and use of the Deliverables and for determining whether to use or refrain from using any recommendation that may be made by Accenture and (viii) the Client will be solely responsible for determining whether any Services provided by Accenture (a) meet Client's requirements; (b) comply with all laws and regulations applicable to Client; and (c) comply with Client's applicable internal guidelines and any other agreements it has with third parties.

15. **General:**

15.1 **Entire Understanding and Severability.** This Agreement, including underlying SOWs, sets forth the entire understanding between two sophisticated business entities with legal counsel with respect to its subject matter, and save in respect of fraudulent misrepresentation supersedes all prior agreements, conditions, warranties, representations, arrangements and communications, whether oral or written, and whether with or by Accenture, any of its affiliates, or any of their employees, officers, directors, agents or shareholders. Each party acknowledges that it is entering into this Agreement solely on the basis of the agreements and representations contained herein, and that it has not relied upon any representations, warranties, promises, or inducements of any kind, whether oral or written, and from any source. If a court of competent jurisdiction finds any term of this Agreement to be invalid, illegal or otherwise unenforceable, such term will not affect the other terms of this Agreement and will be deemed modified to the extent necessary, in the court's opinion, to render such term enforceable while preserving to the fullest extent permissible the intent and agreements of the parties set forth in this Agreement.

15.2 **Exhibits.** In the event of a conflict between this Agreement and an SOW, the SOW controls for purposes of that SOW only. This Agreement may include one or more Exhibits at the time of execution which shall be listed and considered part of the Agreement.

15.3 **Changes.** This Agreement (including the Services, Deliverables, timelines and fees in an SOW) may not be modified or amended except by the mutual written agreement of the authorised representatives of the parties carried out in accordance with the agreed procedure in Schedule 1 (*Change Control Procedure*). Any purchase order issued by the Client will be for its administrative purposes only and none of its terms and conditions will be of any force or effect against Accenture.

15.4 **Third Party Rights.** There are no third party beneficiaries to this Agreement.

16. **Assignment.** Neither party may assign this Agreement (other than to a party's UK subsidiary or affiliate) without the prior written consent of the other, which consent will not be unreasonably withheld or delayed.



17. **Notices.** Any notice or other communication provided under this Agreement will be in writing addressed to such party at the address set forth herein.
18. **Excuse.** Neither party will be liable for any delays or failures to perform due to causes beyond that party's reasonable control (including a force majeure event). Without limiting the foregoing, to the extent Client fails to perform one or more responsibilities described in this Agreement, Accenture shall be excused from failure to perform any affected obligations under this Agreement. Each party will notify the other party as promptly as practicable after such party becomes aware of the occurrence of any such condition. If there is any delay, then the periods for completion of the parties' obligations will be automatically extended by the period of such delay.
19. **References.** Neither party will use the other party's name outside its organization without prior express written consent of the other party, which consent may be withheld in its sole discretion. Notwithstanding the foregoing, Accenture shall be permitted to refer to Client as a customer reference concerning the general area of work under this Agreement, for opportunities at existing and prospective Accenture clients. Accenture may request and Client will provide reasonable written or verbal verification of the engagement and general nature of the Services to such Accenture clients (such verification not to be unreasonably withheld). Client's Information and the pricing that Client paid for the Accenture services shall not be disclosed in such referrals without the permission of Client.
20. **Waiver.** No waiver or modification of any provision of this Agreement, including any underlying SOW, will be effective unless it is in writing and signed by the party against which it is sought to be enforced. The delay or failure by either party to exercise or enforce any of its rights under this Agreement is not a waiver of that party's right to later enforce those rights, nor will any single or partial exercise of any such right preclude any other or further exercise of these rights or any other right.
21. **Audit.** Client will have the right to audit, at its expense, and Accenture will provide Client's employees, independent inspection agent and/or their representatives (so long as such inspection agent or representatives are not competitors of Accenture) with reasonable access to Accenture's and its subcontractor's premises (if applicable), personnel, data, records, controls, processes, and procedures relating to Services to be provided by Accenture, for the purpose of determining whether Accenture is in compliance with its obligations under this Agreement until 12 months following termination of this Agreement. Client will provide fourteen (14) days' prior written notice of its intention to conduct such an audit. Client will conduct such audits in a manner that will result in minimal disruption to Accenture's business operations. Audits may be conducted during normal business hours once annually. Client will not be entitled to audit (i) data or information of other customers or clients of Accenture; (ii) any cost information unless such is the basis of a reimbursable expense; (iii) Accenture's quality assurance reviews and contract management reports; (iv) third parties (subcontractors, licensors or vendors of Accenture) except to the extent Accenture has the right to grant the same, or (v) any other Information of Accenture that is not directly relevant for the authorized purposes of the audit. The auditors and other representatives of Client will execute confidentiality agreements prior to such audit and comply with such security requirements as Accenture may require in connection with such audits. If errors are identified by an audit, Accenture shall take prompt action to correct any error.



**AGREED AND ACCEPTED:**

**Accenture Signature**\_\_\_\_\_

**Client Signature**\_\_\_\_\_

**Name and Title:** \_\_\_\_\_

**Name and Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Date:** \_\_\_\_\_

# Schedule 1

## (Change Control Procedure)

### 1. Definitions and interpretation

1.1 In this Schedule, unless otherwise defined, capitalised words and expressions shall have the meaning set out in the Agreement.

1.2 The following capitalised words and expressions have the following meaning:

**“Business Day”**: Monday to Friday (inclusive) except on UK bank and public holidays;

**“Change”**: an amendment to: scope, nature, volume, project specification, Fees, Services or Deliverables under this Agreement and/or the SOW or any term of this Agreement;

**“Change Control Note”** or **“CCN”**: the written record of any Change agreed or to be agreed by the parties pursuant to the Change Control Procedure;

**“Change Control Procedure”**: the procedure for agreeing a Change set out in this Schedule 1;

**“Dispute Resolution Procedure”**: the procedure for resolving any dispute under or in connection with this Agreement or the SOW as set out in Section 12 of the Agreement; and

**“Fees”**: the fees payable to Accenture for the Services pursuant to the Agreement.

2. Where Accenture or Client wishes to make any Change, the party wishing to make the Change shall discuss the Change with the other party and such discussion shall result in either: (i) a written request for a Change by Client; or (ii) a written recommendation for a Change by Accenture; or (iii) if neither party wishes to submit a request or recommendation, the proposal for the Change will not proceed.
3. Where a written request for a Change is received from Client, Accenture shall, unless otherwise agreed, submit a CCN to the Client within the period agreed between them or, if no such period is agreed, within five (5) Business Days from the date of receipt of such request for a Change.
4. Where Accenture wishes to make a Change, Accenture shall submit a written recommendation for the Change as a CCN direct to Client at the time of such recommendation and Client will confirm receipt of such CCN within five (5) Business Days and the Parties will agree next steps. Neither party shall be obliged to accept any request for Change made by the other and shall have no liability for failing to do so.
5. Each CCN shall contain:
  - 5.1 the title of the Change;
  - 5.2 the originator and the date of the request or recommendation for the Change;
  - 5.3 the reason for the Change;
  - 5.4 the full details of the Change, including any specifications and user facilities;
  - 5.5 the price, if any, of or associated with the Change;
  - 5.6 a timetable for implementation, together with any proposals for acceptance of the Change;
  - 5.7 the impact, if any, of the Change on other aspects of this SOW, including:
    - 5.7.1 the price,
    - 5.7.2 the contractual documentation, and
    - 5.7.3 staff resources;
  - 5.8 the date of expiry of validity of the CCN (which shall not be less than twenty (20) Business Days); and
  - 5.9 provision for signature of the CCN by Client and Accenture.
6. For each CCN submitted, Client shall, within the period of validity of the CCN:
  - 6.1 allocate a sequential number to the CCN;
  - 6.2 evaluate the CCN, and as appropriate either (i) request further information, or (ii) approve the CCN, or (iii) notify Accenture of the rejection of the CCN; and
  - 6.3 if approved, arrange for two copies of the approved CCN to be signed for or on behalf of Client and Accenture. The signing of the CCN shall signify acceptance of a Change by both Client and Accenture.

7. Once signed by Client and Accenture, the Change shall be immediately effective and Client and Accenture shall perform their respective obligations based on the agreed amendment.

## Exhibit A (Statement of Work)

Accenture (UK) Limited whose registered office is located at 30 Fenchurch Street, London EC3M 3BD (“**Accenture**”) will provide the services (“**Services**”) and deliverables (“**Deliverables**”) listed in this agreement to [Client Entity] whose registered office is located at [Client Address] (“**Client**”) as specified below and under the Master Services Agreement (“**MSA**”) signed between the Parties and dated [Date of MSA] (collectively the “**Agreement**”).

### **1.0 Background & Project Description**

The Client is undertaking a [Project Description] (the “**Project**”). The Client has engaged Accenture to provide Services and Deliverables to assist with the Project.

### **2.0 Services and Deliverables**

#### **2.1 Services**

Accenture will provide the following Services to assist the Client with the Project.

[Services Description]

#### **Out of Scope**

The Client acknowledges and agrees:

- [conducting or executing any configuration or system checks/testing/verification across any applications or server infrastructure and/or network appliances is excluded from the Services;]
- all cyber defense services (such as penetration testing, vulnerability testing, adversary simulation, threat hunting, or incident response) are excluded from the Services;
- Accenture will not advise or ensure Client is compliant with any security or other application standards;
- Accenture will not advise or ensure that Client is compliant with any legal, regulatory, industry or internal requirements, standards or policies;

and for the avoidance of doubt, any item of scope which is not stated clearly in this Agreement as in scope is deemed out of scope.

#### **2.2 Deliverables**

The following deliverables (“**Deliverables**”) will be produced by Accenture and the Client (“**Project Team**”) further described in Section 3 below.

<b>Deliverables*</b>	<b>Description (detailed description including format of deliverable)</b>	<b>Accenture Responsibility</b>	<b>Client Responsibility</b>
[XX]	[XX]	[XX]	[XX]

\*Accenture as the party with “primary” responsibility shall have the obligation of completing the tasks necessary to create the above defined Deliverables. The Client shall “assist” Accenture in meeting their primary responsibilities by providing timely access to applicable data, tools, systems, documentation, resources and third parties necessary for Accenture to fulfil their primary responsibilities.

The acceptance criteria for the Deliverables developed by Accenture shall be compliance to the Deliverable description set forth in the table above, or such other acceptance criteria as the parties may agree to in writing subject to a Change Order. The only basis for acceptance of Deliverables will be material compliance to such description or acceptance criteria, in accordance with the acceptance procedures in Section 4 of the MSA. The only basis for rejection of Deliverables will be the failure of the Deliverables to materially comply to such description or acceptance criteria, in accordance with the acceptance procedures in Section 4 of the MSA.

Unless otherwise agreed to in writing by the parties, the above describes Accenture’s complete scope of Services.

### **3.0 Project Location, Timing, and Staffing**

#### **3.1 Project Location**

The Services will be performed at Client’s facilities at [enter location] and/or Accenture’s facilities.

#### **3.2 Timing**

The Services will commence on [xxx]. The estimated timeframe established for performance of the Services will be [xxx] calendar months from commencement date and is further described in the table below:

### **3.3 Staffing/Project Team**

#### **3.3.1 Project Team**

##### **Accenture:**

Accenture's overall Services will be led by [xxx]. Day to day engagement responsibility will be led by [xxx].

##### **Client:**

The Project will be under the control of [xxx], [title], supported by additional Client personnel as appropriate.

### **4.0 Client Obligations and Assumptions**

In addition to any other responsibilities or assumption described in this Agreement, set forth below is a list of the obligations for which Client will be responsible, conditions on Accenture's performance, and assumptions upon which Accenture relies in agreeing to perform the Services described in this Agreement on the terms set out herein (collectively "Client Obligations"). If any of Client's Obligations are not performed or prove to be incorrect, it may cause changes to the Project schedule, fees and expenses, Deliverables, level of effort required, or otherwise impact Accenture's performance of the Services described in this Agreement, and Accenture shall have no liability with respect to its inability to perform the Services resulting therefrom. Client shall grant to Accenture such additional time as is reasonable to provide the Services and/or the relevant Deliverables, as the case maybe, and shall pay to Accenture any additional fees necessary to compensate Accenture for any necessary additional effort or expenses. The Client Obligations are as follows:

1. Client will commit the necessary resources and management involvement to support the Project and perform the agreed upon acceptance procedures in Section 4 of the MSA in a timely manner, and who have access to any relevant tools and data required for the Project.
2. [Accenture shall have no access to client Personal Data. Client shall not provide Accenture with any Personal Data.]
3. Decisions to be made by the Client will be made promptly and without delay.
4. Client shall be responsible for obtaining, at no cost to Accenture, consents for Accenture to gain access to any third-party providers involved with the Client's Project, necessary for Accenture to perform its obligations under this Agreement.
5. Client shall ensure that it procures for the benefit of Accenture, all consents and rights necessary from employees, contractors, third party licensors and suppliers required for Accenture to perform the Services and deliver the Deliverables under this Agreement.
6. Client shall be responsible for the performance of other contractors or vendors engaged by Client in connection with the Project and ensuring that they cooperate with Accenture.
7. Any Confidential Information disclosed to third parties contracted by the Client shall be subject to the confidentiality obligations of this Agreement.
8. Client is responsible for its compliance with laws, regulations and standards, and is responsible for determining whether any recommendations made by Accenture will enable compliance by Client with such laws, regulations and standards.

### **5.0 Project Fees and Expenses**

#### **5.1 Project Fees**

[xxx]

#### **5.2 Expenses**

[xxx]

### **6.0 Additional Terms and Conditions**

#### **6.1 Disclaimer**

Any recommendations or advice provided by Accenture in connection with the Services are provided from a business and/or technical perspective only and do not constitute in any way legal advice or recommendations and Client should not rely on them as such.

Client acknowledges that it is responsible for: (a) assessing the applicability to Client's business and operations of the Deliverables and Services and any recommendations, advice or instructions provided by Accenture in the course of providing the Services, and (b) determining whether the Services and Deliverables provided by Accenture, including any revised business processes implemented pursuant to this Agreement to: (i) meet Client's business requirements, (ii) comply with all Client Laws and (iii) comply with Client's applicable internal guidelines, long-term goals and any related agreements.

Accenture is not a law firm or a legal advisor and cannot provide legal opinions or recommendations and Accenture and its personnel are not licensed, certified and/or registered in any jurisdiction as accounting, auditing, bookkeeping or tax advisory professionals. Accordingly, Accenture and its personnel shall not provide any legal, accounting, audit, attest or tax advice whether governed by law or custom.

Client acknowledges that it has knowledge and skill particular to its business practices and it will share such knowledge and skill, and provide Accenture access to Client's subject matter resources, to facilitate the provision of the Services and Deliverables. The Deliverables are intended for Client's own internal use only and not for any use by third parties nor for use in any legal proceedings. Accenture disclaims any liability that may arise out of any third party's review and/or use of such Deliverables, whether in whole or in part and/or any liability arising out of or in connection with such Deliverables being used in legal proceedings. In no circumstances will Accenture be required to provide expert testimony in connection with the provision of the Services under this Agreement.

Additionally, and notwithstanding anything to the contrary in this Agreement, Accenture does not represent, warrant, or covenant that the Services performed under this Agreement will: (a) detect or identify any or all security or network threats to, or vulnerabilities of Client's networks or other facilities, assets, or operations; (b) prevent intrusions into or any damage to Client's networks or other facilities, assets, or operations; (c) meet or help Client meet any industry standard or any other requirements including the payment card industry data security standard.]

## **6.2 Intellectual Property**

Notwithstanding any term to the contrary, Accenture owns all Intellectual Property: (a) of Accenture existing prior to the Services, including, without limitation, in any Materials provided by Accenture in connection with the Services, or (b) licensed to Accenture by third parties and used in the Services, and (c) any enhancements or modifications to, or derivative works of, any Intellectual Property in categories (a)-(b).

For purposes of this Section, the following definitions shall apply:

- **"Intellectual Property"** means unpatented inventions, patent applications, patents, design rights, copyrights, trade marks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights and forms of protection of a similar nature.
- **"Materials"** means any materials, including without limitation, reports, documents, templates, studies, software programs in both source code and object code, specifications, business methods, tools (including, without limitation, the Seven Domain Diagnostics tool), methodologies, processes, techniques, analytical frameworks, algorithms, know-how, processes, products, documentation, abstracts and summaries thereof.

## **6.3 Project Deliverables**

[Client must not amend, modify or otherwise alter any Deliverable prepared by Accenture under this Agreement without Accenture's prior written consent, such consent which can be withheld at Accenture's sole discretion.]

Use of any report or Deliverable is limited to Client, and cannot be relied upon by any third party. Accenture will not be liable for Client's disclosure of any report or Deliverable or the information in it to, or their use by, any third party.

## Exhibit B (Certus Support Services)

**THIS STATEMENT OF WORK** ("SOW") is made and entered into upon the [date] day of [month and year];

### BETWEEN:

1. [Name of the client], a company incorporated in [country] with registration number [number] and registered office [registered office address] (the Client); and
2. **ACCENTURE (UK) LIMITED** a company incorporated in England whose registered office is at 30 Fenchurch Street, London EC3M 3BD (the "**Service Provider**");

The above named shall collectively be known as "Parties", and each a "Party".

### WHEREAS:

- (A) The Parties have entered into a Master Services Agreement (the "**MSA**") for the provision of certain services by the Service Provider to the Client dated [date of the master services agreement] (the "**Agreement**").
- (B) The Client wishes to instruct the Service Provider to provide the Services (and the Service provider wishes to provide the Services) on the terms and conditions of this Statement of Work and the terms and conditions of the Agreement.

**IT IS HEREBY AGREED** as follows:

### 1 Definitions and Interpretation

- 1.1 In this Statement of Work, unless expressly stated to the contrary, all defined terms shall have the meaning set out in the Agreement.
- 1.2 This Statement of Work expressly incorporates the terms of the Agreement.
- 1.3 Additionally, the following definitions shall apply:
  - 1.3.1 "24 X 7" shall mean 24 hours per day, 7 days per week, 52 weeks per year.
  - 1.3.2 "ADDITIONAL CHARGE" shall mean a charge levied by Service Provider for activities which are outside the scope of SUPPORT, such charge being agreed by Service Provider and Client prior to any such activity commencing.
  - 1.3.3 "CALL-OFF TIME" shall mean the time used for the delivery of services which are outside the scope of the fixed price service, as referenced in clause **Error! Reference source not found.** of this SOW.
  - 1.3.4 "CALL-OFF UNITS" shall mean the unit of allocation for CALL-OFF TIME. CALL-OFF UNITS will be used by Client at a rate which is defined in clause **Error! Reference source not found.** of this SOW.
  - 1.3.5 "CAPPED INCIDENTS" – do not apply to this SOW.
  - 1.3.6 "CHANGE REQUEST" shall mean a request to effect a permanent change to the configuration of a SUPPORTED SYSTEM. Changes are managed in accordance with the CHANGE MANAGEMENT PROCESS.
  - 1.3.7 "CHANGE MANAGEMENT PROCESS" shall mean the agreed process for management of a CHANGE REQUEST as defined within this SOW.
  - 1.3.8 "DEFECT" shall mean any fault within a SUPPORTED SYSTEM which is contrary to the agreed and documented system specification; has been released in line with the CHANGE MANAGEMENT PROCESS and RELEASE MANAGEMENT PROCESS; and is not an IMPLEMENTATION PROJECT WARRANTY REQUEST.
  - 1.3.9 "IMPLEMENTATION PROJECT WARRANTY REQUEST" shall mean any system defect, application software code or configuration fault, or change request which is identified prior to or during a warranty period as defined within a separate Statement of Work or other such agreement between Client and Service Provider pertaining to the implementation of or enhancement to SUPPORTED SYSTEMS.
  - 1.3.10 "INCIDENT" shall mean a fault within a SUPPORTED SYSTEM. INCIDENTS are managed in accordance with the INCIDENT MANAGEMENT PROCESS.
  - 1.3.11 "INCIDENT MANAGEMENT PROCESS" shall mean the agreed process for management of an INCIDENT as defined within this SOW.
  - 1.3.12 "NORMAL WORKING DAY" shall mean GMT Monday to Friday, excluding UK bank holidays.



- 1.3.13 "PROBLEM" shall mean the root cause of one or more INCIDENTS within a SUPPORTED SYSTEM. PROBLEMS are managed in accordance with the PROBLEM MANAGEMENT PROCESS.
- 1.3.14 "PROBLEM MANAGEMENT PROCESS" shall mean the agreed process for management of a PROBLEM as defined within this SOW.
- 1.3.15 "RELEASE" shall mean the movement of configuration items from one SUPPORTED SYSTEM to another. RELEASES are managed in accordance with the RELEASE MANAGEMENT PROCESS.
- 1.3.16 "RELEASE MANAGEMENT PROCESS" shall mean the agreed process for management of a RELEASE as defined within this SOW.
- 1.3.17 "REMOTE ACCESS" shall mean the method of accessing Client systems using Service Provider's standard site-to-site Virtual Private Network (VPN) access method.
- 1.3.18 "SERVICE QUARTER" shall mean the three month period commencing from the first day of the calendar month following the SUPPORT COMMENCEMENT DATE and every three calendar month period thereafter.
- 1.3.19 "SUPPORT" shall mean the support services provided by Service Provider to Client under this SOW.
- 1.3.20 "SUPPORT ANNIVERSARY DATE" shall mean the SUPPORT END DATE and each anniversary thereafter until such time as the SOW is terminated in accordance with clause **Error! Reference source not found.** of this SOW.
- 1.3.21 "SUPPORT COMMENCEMENT DATE" shall mean the commencement date of the ongoing support services described in this SOW and is defined as: <dd month yyyy>
- 1.3.22 "SUPPORT END DATE" shall mean the date which is 36 (thirty-six) calendar months after the SUPPORT COMMENCEMENT DATE.
- 1.3.23 "SUPPORT HOURS" shall mean the times in which the SUPPORT is delivered, as defined in section **Error! Reference source not found.** of this SOW.
- 1.3.24 "SUPPORTED SYSTEMS" shall mean those systems listed within this SOW which are subject to SUPPORT.

## 2 Description of Services

This SOW describes the details of the <enter comma-separated list of service disciplines here eg. "Oracle Fusion HCM Functional Support, Oracle Taleo Recruit Functional Support"> support agreement between Service Provider and Client.

- Section 3 of this SOW defines the services being delivered.
- Section 4 defines the Service Management approach and the related SERVICE LEVEL AGREEMENT ("SLA").
- Section 5 details the Fees and Charges associated with this service.

## 3 Services to be provided

The following services shall be provided under this SOW.

- 3.1 This SOW covers the provision of <enter comma-separated list of service disciplines here eg. "Oracle Fusion HCM Functional Support, Oracle Taleo Recruit Functional Support"> support services to Client.
- 3.2 Client has deployed the following services components: <enter comma-separated list of service components here eg. "Oracle Fusion HCM Cloud Service, Oracle Release 11.5.9 General Ledger or Accounts Payable Modules">.
- 3.3 Support is primarily provided via REMOTE ACCESS. On-site support may be provided on a case by case basis only if agreed in advance by both Service Provider and Client.
- 3.4 This SOW covers the provision of support for a maximum of Production, plus a maximum of non-Production for each Production .
- 3.5 Any changes to the scope as defined within this SOW, including but not limited to the number of supported environments, software components or system architecture, will be subject to the change control process set forth in the Agreement and a review of the costs of providing the services defined within this SOW.
- 3.6 Overall Service Parameters

The following table contains an inventory of the general service parameters in respect of the SOW.

Component	Service Scope
Telephone, email and Internet portal access to Service Provider Service Desk for logging of an INCIDENT, PROBLEM or CHANGE REQUEST.	
Named Service Delivery Manager.	
Dedicated Service Provider Client Gateway document management portal.	
REMOTE ACCESS for Service Provider management of INCIDENT, PROBLEM and CHANGE REQUEST.	

3.7 Service Element: <Enter service elements such as Oracle Fusion HCM functional and technical support, Taleo functional support etc>

The following clauses define the scope of the **Error! Reference source not found.** services.

3.7.1 **Error! Reference source not found.** - Incident and Problem Management.

The following table defines the Incident and Problem Management service parameters for the <enter service elements> service element, which are carried out in accordance with the INCIDENT MANAGEMENT PROCESS and PROBLEM MANAGEMENT PROCESS.

Component	Service Scope
Fix-On-Fail support for INCIDENTS reported by Client on SUPPORTED SYSTEMS.	
"How to" advice relating to SUPPORTED SYSTEMS.	
Unit testing of Vendor software patches in direct response to INCIDENTS on SUPPORTED SYSTEMS.	
System Administration for the SUPPORTED SYSTEMS (e.g. user, responsibility, profile, menu setups)	
"PatchAware" service offering relating to Fusion HCM and Taleo version upgrades for the SUPPORTED SYSTEMS	

3.7.2 **Error! Reference source not found.** - Change and Release Management

The following table defines the Change and Release Management service parameters for the **Error! Reference source not found.** element. These will be carried out in line with the CHANGE MANAGEMENT PROCESS and RELEASE MANAGEMENT PROCESS.

Component	Service Scope
Business process impact assessment related to the application of mandatory, legislative or regulatory database patches	
Any testing required to ensure the patch has been applied in line with Vendor's recommendations	
Changes to business processes and procedures and resultant required changes to ERP structures (for example: Workflow processes) as a result of the application of vendor patches	
Minor changes / enhancements to currently deployed ERP solution.	

### 3.8 Additional Services

3.8.1 Additional support activities which are not included in the standard service defined above, can be provided by way of CALL-OFF TIME or subject to ADDITIONAL CHARGE, on request from the Client, as defined in clauses **Error! Reference source not found.** and **Error! Reference source not found.** of this SOW.

### 3.9 Sarbanes-Oxley Disclaimer

During this engagement Service Provider may perform services that Client has requested in connection with Client's compliance with the Sarbanes-Oxley Act and related regulations (collectively, "Sarbanes-Oxley"). Sarbanes-Oxley compliance is the responsibility of Client. Service Provider is not being engaged to provide assurance as to Client's compliance with Sarbanes-Oxley or to determine any deficiencies in Client's internal controls or financial reporting, or to disclose financial statement errors, irregularities or illegal acts. Service Provider's services are not designed and cannot be relied upon to determine Client's compliance with Sarbanes-Oxley, and Service Provider shall have no responsibility or liability for or in connection with such compliance.

## 4 Service Management

The following clauses define the service terms and conditions and Service Level Agreement commitments, together with a description of the Service Provider service engagement processes to include service transition and on-going service management.

### 4.1 Term and Termination

- 4.1.1 This SOW shall commence on its SUPPORT COMMENCEMENT DATE and shall continue until its SUPPORT END DATE.
- 4.1.2 This SOW may be terminated by Client by giving 3 (three) months written notice within 30 (thirty) days of Non Performance as defined in clause **Error! Reference source not found.** of this SOW.
- 4.1.3 This SOW will survive any termination of the associated Agreement and the terms of the Agreement will continue to apply in full to this SOW until this SOW is terminated according to this clause 4.1. This clause 4.1.3 takes precedence over any implied or explicit provisions in the associated Agreement that would cause a SOW to be terminated concurrently with the termination of the Agreement.
- 4.1.4 Clause 4.1.3 will not apply only where termination of the Agreement is a direct result of provisions in the Agreement relating to either party becoming bankrupt or making any arrangement with its creditors, becoming insolvent, entering into receivership or liquidation, taking any action for voluntary winding-up otherwise than for the purpose of a solvent reconstruction or amalgamation or ceasing to carry on business.

### 4.2 Non Performance

- 4.2.1 The key service performance indicators ("KPIs"), and associated Target Compliance level, for this SOW are defined in Clause **Error! Reference source not found.**

- 4.2.2 Service Provider shall not be deemed to have failed to perform against the KPIs if such failure arises from a breach by Client of its obligations as defined within this SOW, or from force majeure.
- 4.2.3 If Service Provider fails to meet any KPI over any given SERVICE QUARTER then the Client must inform Service Provider in writing within thirty (30) days of the end of the SERVICE QUARTER of this non-compliance.
- 4.2.4 [If Service Provider fails to meet any KPI Target Compliance in consecutive SERVICE QUARTERS (“Non Performance”), then the Client shall be entitled to terminate the SOW as per clause **Error! Reference source not found.**, provided that Client has previously served the notice referred to in clause **Error! Reference source not found.** in respect of failures to meet KPIs which give rise to the right to terminate.]

#### 4.3 Support Service Transition

##### 4.3.1 Where Service Provider has not implemented the system to be supported:

- a) A system review will be performed by Service Provider to assess the status of the SUPPORTED SYSTEMS, and to review corresponding documentation as part of this SOW. Service Provider may make reasonable recommendations that arise out of this exercise, taking into consideration the Client’s plans for the SUPPORTED SYSTEMS. These will be discussed with the Client, and subject to the Client’s approval, these may result in the need for additional activities, delivered subject to ADDITIONAL CHARGE or through the use of CALL-OFF TIME.
- b) In cases where any of the SUPPORTED SYSTEMS do not meet the entry level criteria for the on-going support service as defined within this SOW, Service Provider will advise Client, in writing, of the required remedial activity. Such criteria include, but are not limited to:
  - minimum recommended patch levels as dictated by the respective software vendor;
  - validated under-pinning third party support agreements where appropriate;
  - remedying any current configuration errors which will become subject to the on-going support commitments.
- c) Until such work has been undertaken Service Provider will provide on-going support on a reasonable endeavours basis. In such cases, and also in cases where Vendor support is no longer available for the deployed solutions/versions, Service Provider will not be liable for any commitments under the Service Level Agreement in respect of the individual system within SUPPORTED SYSTEMS.

##### 4.3.2 In all cases, irrespective of whether Service Provider has implemented the system to be supported:

- a) A Service Delivery Plan is produced. The Service Delivery Plan is intentionally non-contractual and contains explanations of the most effective use of Incident, Problem, Change and Release Management processes and supporting systems.
- b) The support infrastructure is configured. This includes:
  - (i) Setting up and testing of REMOTE ACCESS, where deployed.
  - (ii) Configuration and testing of Service Provider call logging software, to include the creation of up to named user accounts for Client employees from whom Service Provider will accept support requests.
- c) The support procedures are communicated internally within the Client and any required training is provided in such support procedures by Service Provider. The support procedures are tested so the transition can be as seamless as possible.
- d) The transition into the ongoing support service is undertaken on the SUPPORT COMMENCEMENT DATE, so that any outstanding issues or change requests will be detailed and transferred to the support service as described in this SOW.

#### 4.4 The Provider Service Desk

- 4.4.1 The Service Provider Service Desk can be contacted by telephone, email or Internet based portal for the logging of an INCIDENT, CHANGE REQUEST or “How To” advice and guidance.
- 4.4.2 All communication between Client and Service Provider will be in English language and any requirement to translate data; labels; boilerplate text; documentation; user instructions or other such system elements into English will be undertaken by Client.
- 4.4.3 Escalation Procedure

- e) INCIDENTS are automatically escalated within Service Provider's support team as they progress through the INCIDENT MANAGEMENT PROCESS. Should the Client be unhappy about the quality of service provided at any point they should contact the designated Service Provider personnel as defined within the Service Delivery Plan.

#### 4.5 Service Delivery Management

4.5.1 Where stated within clause **Error! Reference source not found.** of this SOW, Service Provider will allocate a Service Delivery Manager ("SDM") to the Client. The SDM will undertake the following activities:

- f) Will undertake a support process review. Service Provider's support processes are reviewed with the Client and modified where reasonable to integrate with the Client's internal procedures. The resulting procedures are documented within the Service Delivery Plan.
- g) Will act as prime point of escalation for the Client for operational matters relating to the support service defined in this SOW.
- h) Will produce a support Service Review report on a basis and circulate this to the designated Client contacts. The report will detail INCIDENTS logged, resolved and open; together with key performance indicator information. Where applicable to this AGREEMENT the report will also include utilisation reports on the usage of CALL-OFF TIME and CAPPED INCIDENTS.
- i) Will attend up to a maximum of Service Review meetings (xx) per annum with the designated Client relationship manager. This meeting will consider the activities that have taken place in the previous period, areas for improvement, lessons learnt and planned activities for the next period.

#### 4.6 The Incident Management Process

4.6.1 The INCIDENT MANAGEMENT PROCESS is the Service Provider process governing the return to operation of a SUPPORTED SYSTEM which has developed a fault. An INCIDENT is deemed resolved when service has been restored to the end user.

4.6.2 Where Service Provider restores service by way of a temporary work-around, the PROBLEM MANAGEMENT PROCESS may be invoked to investigate and address the root cause. Problem Management will only be invoked as the result of an INCIDENT being raised.

4.6.3 Where a permanent change is required to a SUPPORTED SYSTEM as the result of an INCIDENT, Service Provider may invoke the CHANGE MANAGEMENT PROCESS to effect such change. The CHANGE MANAGEMENT PROCESS may be invoked without the need for an initial Incident to be raised.

4.6.4 The Severity of an INCIDENT is important since it determines the level of service offered. The INCIDENT will be assigned a Severity Level at the time it is first placed in accordance with the following guidelines:

Severity	Definition
Urgent	A Production SUPPORTED SYSTEM is unavailable to all users, or a business-affecting security breach - or suspected security breach - has occurred.
High	A Production SUPPORTED SYSTEM is available but all users are experiencing degraded service performance, which is impacting on Client's business operations.
Normal	Any INCIDENT affecting on-going service which is not deemed Severity 1 or Severity 2 Any INCIDENT on a Production SUPPORTED SYSTEM affecting a single user. Any INCIDENT relating to Non-Production servers and associated services. This is the default INCIDENT severity.
Low	Any request which does not warrant a higher Severity INCIDENT, for example: <ul style="list-style-type: none"> <li>o An intermittent fault affecting a single user where an acceptable workaround is available.</li> <li>o "How to" advice.</li> </ul>

4.6.5 The Client shall allocate a Severity level to each INCIDENT raised in line with the definitions stated above. Service Provider will review this INCIDENT setting during initial triage activities and as the INCIDENT diagnosis and any associated remedial work progresses.

- 4.6.6 The INCIDENT Severity may be upgraded or downgraded in situations where the impact on Client's business changes, any such amendments being reflected in the respective Incident record.

In cases where Client upgrades the Severity of an existing INCIDENT, such action may result in the INCIDENT causing a failure to achieve the under-pinning Service Level Agreement due to time having already elapsed on the previous Severity level. In such cases the INCIDENT will be excluded from the Service Level Agreement compliancy calculations, however Service Provider will acknowledge the heightened Severity level and use reasonable endeavours to ensure the INCIDENT is resolved in line with the new Severity definition.

If Client wishes to retain SLA calculations for an upgraded Severity Incident, Client should resolve the existing INCIDENT and create a new INCIDENT at the upgraded Severity cross-referencing the two INCIDENT records for clarity and audit purposes.

In cases where the Severity of an Incident is downgraded, there is no requirement to raise new INCIDENT records and the SLA calculations will be re-calibrated as appropriate.

#### 4.6.7 Incident Progression

- a) On receipt of an INCIDENT, Service Provider will instigate one or more of the following actions:
  - o Assign ownership of the INCIDENT to a second level specialist support group, notifying Client of such actions.
  - o Investigate the INCIDENT and decide future course of action.
  - o Request further information from the Client where necessary.
  - o Provide advice to Client for resolution of the INCIDENT or provide workarounds.
  - o Regularly update the ServiceDesk Portal to advise the Client of progress.
- b) For INCIDENTS that result in a Vendor (for example Microsoft or Oracle) Service Request, Service Provider may progress these on behalf of the Client, where this has been agreed with Client.
- c) On resolution of an INCIDENT, Service Provider will request approval from the Client that it can be closed.
- d) Prior to closure of an INCIDENT, the root causes shall be investigated and appropriate actions shall be raised by Service Provider, invoking the PROBLEM MANAGEMENT PROCESS where appropriate.

#### 4.6.8 Service Level Agreement

- e) The INCIDENT Management Service Level Agreement ("SLA") defined within this clause 4.10.8 shall constitute a KPI. The SLA shall apply to INCIDENTS which are classified as faults within the SUPPORTED SYSTEM. Service Provider shall respond to such INCIDENTS within the following parameters.

Severity Level	Time to Respond (Note 1)	SUPPORT HOURS
Urgent	xx	xx
High	xx	xx
Normal	xx	NORMAL WORKING DAY
Low	6 hours	NORMAL WORKING DAY

- f) Note 1: A Response is deemed to have occurred when a non-automated human response is provided stating, by way of an update to the INCIDENT record, which of the actions defined within clause **Error! Reference source not found.** Incident Progression has been instigated.
- g) All Service Level targets are measured per SERVICE QUARTER during the stated SUPPORT HOURS for the respective Severity Level.

- h) Target Compliance is calculated as: the percentage of INCIDENTS reported during each SERVICE QUARTER which achieve the specific SLA adherence targets. Where fewer than 10 (ten) INCIDENTS are reported, the calculation is carried forward to subsequent SERVICE QUARTER ends until there are 10 or more INCIDENTS available for the KPI calculation. The Target Compliance shall be set at .
- i) The SLA commitments cannot be adhered to and will not apply in cases where the INCIDENT is caused by the negligent or incorrect actions of Client or other non-Service Provider employee or subcontractor, or where an INCIDENT is the result of problems arising from the illegal usage of the system. Service Provider reserves the right to charge Client for resolving such INCIDENTS subject to ADDITIONAL CHARGE or through the use of CALL-OFF TIME.
- j) Due to their nature, PROBLEM and CHANGE REQUESTS are not subject to this Service Level Agreement.
- k) In cases where Service Provider requires Vendor support to resolve an INCIDENT, and such Vendor support is no longer available, Service Provider will not be liable for any commitments under the Service Level Agreement. In such cases Service Provider will use reasonable endeavours to resolve the INCIDENT but shall not be liable under the SLA commitments.
- l) Elapsed times are measured as the total amount of time during SUPPORT HOURS that any INCIDENT is assigned to Service Provider up to the point of SLA compliance. This excludes any time where Service Provider is waiting for Client or any 3rd party to carry out an activity on which Service Provider is dependent; or time where Client and Service Provider have agreed that an INCIDENT can be set to PENDING awaiting further activity.
- m) Client must notify Service Provider of Urgent Severity and High Severity INCIDENTS by telephone in addition to any portal or email communications. The elapsed time calculations will not commence until Service Provider has been notified of such INCIDENTS by telephone and an INCIDENT has been successfully logged within the ServiceDesk system.
- n) The time taken to restore files from tape or other such media is excluded from the resolution time.
- o) If physical on-site attendance is required at Client or other non-Service Provider premises, then travel time is excluded from the resolution time.
- p) All Service Level Agreement commitments are dependent upon Client complying with the obligations stated within this SOW and elsewhere within the Agreement.
- q) Any INCIDENTS, PROBLEMS or other such support requests directly resultant from or pertaining to an unresolved IMPLEMENTATION PROJECT WARRANTY REQUEST are excluded from SUPPORT and will be catered for under the terms of any such project warranty as defined within the respective project contractual terms. Client may register any related INCIDENTS within the Service Provider Service Desk system but these will be addressed under the provisions of the respective project warranty conditions and not under the terms of SUPPORT.

#### 4.7 The Problem Management Process

- 4.7.1 Where Service Provider restores service by way of a temporary work-around, the PROBLEM MANAGEMENT PROCESS may be invoked to investigate and address the root cause. The PROBLEM MANAGEMENT PROCESS will only be invoked as the result of an INCIDENT being raised.
- 4.7.2 PROBLEM records will be managed within the Service Provider ServiceDesk portal and Client will have the ability to track and review progress against PROBLEM records.
- 4.7.3 Service Provider will inform Client of updates to PROBLEMS, including the eventual resolution and closure activities by way of updates to the PROBLEM record.
- 4.7.4 Where a permanent change is required to a SUPPORTED SYSTEM, Service Provider may invoke the CHANGE MANAGEMENT PROCESS to effect such change.

#### 4.8 The Change Management Process shall be the Change Control Procedure set out in the MSA.

#### 4.9 The Release Management Process

- 4.9.1 The Release Management Process shall be agreed between Service Provider and Client during the Service Transition Process, and shall be as defined in the Service Delivery Plan.



4.9.2 Except where included within the scope of an individual CHANGE REQUEST, the release management of application customisations is not included within the SOW but can be provided using CALL-OFF TIME or subject to ADDITIONAL CHARGE.

#### 4.10 Call-Off Time

4.10.1 Where this service includes CALL-OFF TIME, the associated charges are stated within Clause **Error! Reference source not found.** of this SOW.

4.10.2 CALL-OFF TIME will be allocated in the form of CALL-OFF UNITS. Client can utilise CALL-OFF UNITS to request <INSERT ACTIVITIES HERE> services which are outside the scope of the fixed price SUPPORT defined within this SOW. The rate at which the CALL-OFF UNITS will be deducted from the Client allocation is determined by the individual resource skills-set. The following Table defines [xxx] of CALL-OFF TIME used. For part-days the CALL-OFF UNITS are deducted in line with clauses **Error! Reference source not found.** and **Error! Reference source not found.** of this SOW.

Resource Type	Unit Rate (per eight hour day)
Junior Support Consultant	xx
Support Consultant (Oracle Functional/Technical Consultant incorporating E-Business Suite, Fusion and Taleo) Designer / Developer (Java, Oracle, etc.)	xx
Senior Developer (Oracle SOA, BI, Middleware developer) Senior Consultant / Designer, Project Manager	xx
Solutions Architect / Programme Manager	xx

4.10.3 Where the work is performed remotely it will be called off in increments with a minimum of per request.

4.10.4 Where the work is performed on-site, it will be called off in hour increments, such time to include travelling time to/from Client site. On-site work will be of reasonably incurred expenses.

4.10.5 When CALL-OFF TIME is used outside of a NORMAL WORKING DAY during Monday to Friday, excluding UK Public Holidays, then time will be consumed at 1.5 (one and a half) times the actual CALL-OFF UNITS used.

4.10.6 When CALL-OFF TIME is used during Saturday or Sunday or UK Public Holidays, then time will be consumed at 2 (two) times the actual CALL-OFF UNITS used.

4.10.7 CALL-OFF TIME is subject to a minimum of 2 (two) working days' notice and also subject to Service Provider resource availability.

4.10.8 Unused CALL-OFF UNITS can be carried forward between support years, such years commencing on the SUPPORT COMMENCEMENT DATE and on each anniversary of the SUPPORT COMMENCEMENT DATE thereafter.

4.10.9 Client may claim a partial refund of unused CALL-OFF TIME at the end of the SOW where the time is not rolled forward to a subsequent SOW between Service Provider and Client. Unused CALL-OFF TIME will be refunded at the rate of £ per complete unused CALL-OFF UNIT. No greater than % of the total CALL-OFF UNITS available during the final year of the SOW will be refunded.

#### 4.11 Capped Incidents

4.11.1 CAPPED INCIDENTS do not apply to this SOW.

#### 4.12 Additional Work

4.12.1 Any additional support work that is requested which is outside the scope of this SOW will be undertaken subject to ADDITIONAL CHARGE or via the use of CALL-OFF TIME.

4.12.2 Additional Work which is performed at ADDITIONAL CHARGE is subject to a minimum of [xxx] working days' notice from the receipt of an authorised Client order, and also subject to Service Provider resource availability.

## 5 Fees and Charges

### 5.1 Fixed Fee Elements

Service Element	Amount	Invoice Milestone
Service Transition	xx	xx
Annual Support Charge	xx	xx
Initial Call-Off Time (where applicable) Number of Units	Amount	Invoice Milestone
xx	xx	xx

5.1.1 Additional CALL-OFF TIME can be purchased at the following rate(s), subject to submission of a duly authorised Client Purchase Order.

Number of Units	Amount	Invoice Milestone
x	xx	
x	xx	
x	xx	

### 5.2 Initial Capped Incidents (where applicable)

#### 5.2.1 CAPPED INCIDENTS do not apply to this SOW.

The parties hereby confirm their agreement to enter into this STATEMENT OF WORK on the terms of the Agreement.

#### AGREED AND ACCEPTED:

Client Signature\_\_\_\_\_

Accenture Signature\_\_\_\_\_

Name and Title: \_\_\_\_\_

Name and Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

## Exhibit C (General Accenture Cloud Service Terms and Conditions)

[Due to constraints in uploading multiple documents, we have consolidated these into one document. In the event of provision of AWS, the AWS Service Order would apply, in the event of provision of Microsoft Azure, the Microsoft Azure Service Order would apply and in the event of provision of Google Cloud, the Google Cloud Service Order terms would apply.]

### 1 AGREEMENT STRUCTURE AND INTERPRETATION

- 1.1 The following General Accenture Cloud Service Terms and Conditions ("Cloud Service Terms") entered into between [Accenture entity] ("Accenture") and [client name] ("Client"), together with the terms of the applicable Service Order, shall govern the provision of Cloud Services by Accenture, and the consumption of Cloud Services by Client. These Cloud Service Terms and together with the individually executed Service Order(s) (and any appendices attached thereto) shall each collectively form a "Cloud Agreement".
- 1.2 The Cloud Agreement shall govern the provision and consumption of Cloud Services, to the exclusion of any other terms and conditions. The terms and conditions of the [Master Service Agreement] entered into by the Parties on [add date] shall explicitly not govern or apply in any manner to the provision or consumption of Cloud Services, unless otherwise stated hereunder.
- 1.3 If there is a conflict or inconsistency between these Cloud Service Terms and a Service Order, the Service Order shall prevail to the extent of the conflict or inconsistency.
- 1.4 Capitalized terms used in these Cloud Service Terms shall have the meaning given to them under the attached Appendix A.

### 2 PROVISION OF CLOUD SERVICES

- 2.1 Accenture shall provide the Cloud Services to Client in accordance with the Cloud Agreement.
- 2.2 Accenture grants to Client a non-exclusive, non-transferable right during the term of the applicable Service Order to access and use (and permit Users to access and use) the Cloud Services, in accordance with the Cloud Agreement.
- 2.3 Client may access and use the Cloud Services for its own internal business purposes only. Client agrees that it shall not license, sub-license, sell, resell, transfer, assign, distribute or otherwise commercially exploit the Cloud Services by making them available for access or use by any third-party that is not a User.
- 2.4 Accenture will use generally accepted industry standard security technologies in providing the Cloud Services as determined by Accenture. More detailed data processing and security policies, if any, shall be included in the applicable Service Order.
- 2.5 Accenture shall perform the Cloud Services in compliance with Applicable Laws that directly pertain to Accenture as a provider of the Cloud Services.
- 2.6 Accenture reserves the right to make updates and changes to the Cloud Services that Accenture deems necessary or otherwise appropriate, provided that Accenture may not make changes to the Cloud Services that would materially reduce or otherwise negatively impact the Cloud Services' core features and functionalities.
- 2.7 Accenture and the Cloud Vendors reserve the right to monitor Client's and Users' access and use of the Cloud Services for the purposes of: (i) obtaining Accenture Insights Data (as defined in Section 4.7 below) to further develop and improve the Cloud Services; and (ii) verifying Client's and Users' compliance with the Cloud Agreement.
- 2.8 Accenture reserves the right to suspend Client's and Users' right to access or use all or any portion of the Cloud Services, or remove any relevant Client Data where Accenture reasonably believes (i) Client or Users are in breach of the Cloud Agreement, including without limitation Section 3.3; (ii) Client has failed to respond to a claim of alleged infringement; or (iii) Accenture is required to do so by Applicable Law, or any court or governmental body order. Accenture also reserves the right to suspend Client's and Users' right to access or use all or any portion of the Cloud Services where Client fails to pay to Accenture any amounts payable within thirty (30) days of such amounts being due.
- 2.9 To the extent permitted by Applicable Law, and if otherwise reasonable and feasible under the circumstances (as determined by Accenture in its discretion), Accenture will provide Client with written notice prior to suspension, and an opportunity to take steps to avoid such suspension. Any suspension or removal of Client Data shall not release Client from its obligations under the Cloud Agreement, including any obligation to pay the fees.

Accenture's suspension right is in addition to Accenture's right to terminate the Cloud Agreement pursuant to Section 10.

- 2.10 Accenture may use Cloud Vendor Solutions in the provision of Cloud Services, in which case Client agrees that Accenture can only provide and make available to Client those Cloud Vendor Solutions included in the Cloud Services under the terms and conditions that the relevant Cloud Vendor has made its Cloud Vendor Solutions available to Accenture. To the extent directly applicable to Client and to the relevant Cloud Services, Cloud Vendor terms shall be incorporated in the relevant Service Order.
- 2.11 Where Accenture uses Cloud Vendor Solutions in the provision of the Cloud Services, Client acknowledges that the Cloud Vendors have reserved the right to change, discontinue and depreciate, or change or remove features or functionalities from, the Cloud Vendor Solutions from time to time. To the extent technically possible and commercially reasonable, Accenture will manage such changes to the Cloud Vendor Solutions so that any impact to the Cloud Services is minimized. Where changes to the Cloud Vendor Solutions would have a material impact on the Cloud Services, Accenture will inform Client as soon as practically possible and at the latest at least [sixty (60) days] in advance of such changes to the Cloud Vendor Solutions coming into force, and enter into good faith negotiations with Client to agree on any necessary changes to the Cloud Services and the Cloud Agreement.
- 3 CLIENT'S RESPONSIBILITIES
- 3.1 Client is solely responsible for determining (a) the suitability of the Cloud Services for its business, and (b) the manner in which Client and its Users access and use the Cloud Services complies with Applicable Law.
- 3.2 Client is responsible for obtaining and maintaining all hardware, software, communications equipment and network connections necessary to access and use the Cloud Services, and for paying any applicable third-party fees and charges incurred to access and use the Cloud Services.
- 3.3 Client shall be responsible for all acts and omissions of Users, as if they were the acts and omissions of Client, and for ensuring that anyone who uses the Cloud Services does so in accordance with the Cloud Agreement. Client shall not, and shall ensure that Users do not:
- (a) take any action or omission that poses a security risk or may otherwise adversely impact the Cloud Services, including by interfering with or disrupting any security controls and mechanisms of the Cloud Services;
  - (b) host or transmit any content, data or information that is illegal, or that infringes any third-party's rights, such as Intellectual Property Rights or right of privacy;
  - (c) take any action or omission that otherwise violates Applicable Law;
  - (d) copy, translate, make derivative works of, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code or underlying ideas or algorithms embodied in the software applications or other systems used in the provision of the Cloud Services, unless expressly permitted under Applicable Law, or remove any titles or trademarks, copyrights or restricted rights notices in the systems, software and other materials used in the provision of the Cloud Services; or
  - (e) access or use (or allow a third party to access or use) the Cloud Services for the purposes of building products or services that are competitive to the Cloud Services.
- 3.4 Except as described in the Cloud Agreement and to the extent that the Parties explicitly have agreed in the Service Order that Accenture will provide any security mechanisms and protections as a service, Client shall be responsible for taking appropriate steps to protect and maintain the security of the Cloud Services and the Client Data, including without limitation:
- (a) backing-up the Client Data to a sufficient standard to ensure Client's business continuity;
  - (b) maintaining commercially reasonable security standards for Users' access to the Cloud Services, including without limitation the use of sufficiently secure passwords and regularly required password changes, and maintaining the confidentiality of any non-public authentication credentials associated with Client's use of the Cloud Services; and
  - (c) using all reasonable endeavors to ensure that Users do not upload or distribute files that contain Viruses, malicious files or other harmful code, or disrupt or attempt to disrupt the systems and networks used in the provision of the Cloud Services, including by using good industry practice virus protection software, and other customary procedures to screen Client Data.
- 3.5 Client shall promptly notify Accenture if it becomes aware of any breach or threatened breach of the terms of Sections 3.3 or 3.4 (b) or (c), or of any breach or threatened breach of security including any attempt by a third

party to gain unauthorized access to the systems used in the provision of the Cloud Services, or any other security incident relating to the Cloud Services.

- 3.6 Client is responsible for responding to any request from a third party regarding Client's use of the Cloud Services, such as a request to take down content under Applicable Law.

#### 4 CLIENT DATA

- 4.1 Client (and Client's licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to the Client Data. Except as provided under the Cloud Agreement, Accenture obtains no other rights to Client Data.
- 4.2 Client acknowledges and agrees that it is solely responsible for the content of all Client Data, and for complying with Applicable Law relating to the Client Data, including without limitation all applicable data privacy and protection laws and regulations. Client will secure and maintain all rights in Client Data necessary for Accenture to provide the Cloud Services to Client, without violating the rights of any third party or otherwise obligating Accenture to Client or to any third party. Client will obtain all required consents from third parties under applicable privacy and data protection laws before providing personal information to Accenture. As and to the extent required by law, Client shall also notify the individual Users of the Cloud Services that their data may be disclosed to law enforcement or other governmental authorities, and Client shall obtain the Users' consent to the same.
- 4.3 Accenture assumes no obligations with respect to Client Data, other than as expressly set forth in the Cloud Agreement, or as required by applicable laws.
- 4.4 Client authorizes Accenture to host, store, process and transfer the Client Data in accordance with the Cloud Agreement, including but not limited to any data processing policy incorporated in or referred to in the applicable Service Order. Client consents to the processing of personal information by Accenture, Cloud Vendors and subcontractors, as required to perform the Cloud Services. Client may choose to provide personal information to Accenture on behalf of third parties (including Client contacts, resellers, distributors, administrators, and employees) as part of this agreement.
- 4.5 Accenture will not disclose Client Data to any third party except: (i) with Client's written consent; (ii) to a Cloud Vendor or a subcontractor to the extent necessary for such Cloud Vendor or subcontractor to provide the Cloud Vendor Solution or subcontractor services respectively; or (iii) as required by Applicable Law, or pursuant to a court order or authorized regulatory body or law enforcement agency.
- 4.6 Client shall have the ability to access its Client Data hosted over the Cloud Services at any time during the term specified in the applicable Service Order. Client may export and retrieve its Client Data during such term, which will be subject to technical limitations caused by factors such as (i) the size of Client's instance of the Cloud Services; and (ii) the frequency and/or timing of the export and retrieval.
- 4.7 Client agrees that Accenture will, notwithstanding any provision in the Cloud Agreement or any Service Order to the contrary, have the right to generate patterns, trends, knowledge, metadata and other insights (i) by anonymizing Client Data; (ii) aggregating Client Data with other data; and/or (iii) based on anonymous learnings, logs and data regarding use of Accenture products and/or services (collectively, "Accenture Insights Data" or "AID"). Accenture Insights Data shall only consist of anonymized data that does not identify Client or contain any Personal Data. Anonymized data means that any information that can identify Client or a natural person is removed and the remaining data is data from which one cannot identify an individual, whether by Accenture or by any other person (i.e., all likely means of re-identification are not possible). The Parties agree that AID shall belong to Accenture, and that Accenture may use AID for any business purpose during or after the term of the Cloud Agreement (including without limitation to develop, provide, operate, maintain, and improve Accenture products and services and to create and distribute reports and other materials).

#### 5 FEES, PAYMENTS AND TAXES

- 5.1 Client shall pay the fees specified in the applicable Service Order. Fees are stated exclusive of all applicable duties, tariffs, and taxes. Unless otherwise specified in a Service Order, fees will be due and payable within thirty (30) days of Accenture's invoice date. Late payments that are not the subject of a good faith dispute are subject to an interest charge, which is the lesser of: (a) one and one-half percent (1.5%) per month, and (b) the maximum rate permissible by Applicable Law.
- 5.2 Client shall provide any information reasonably requested by Accenture to determine whether Accenture is obligated to collect VAT and sales tax from Client, including Client's VAT and sales tax identification number. If Client is legally entitled to an exemption from any sales, use, or similar transaction tax, Client is responsible for providing Accenture with legally-sufficient tax exemption certificates for each taxing jurisdiction. Accenture will apply the tax exemption certificates to charges under Client's accounts occurring after the date Accenture receives the tax exemption certificates. If any deduction or withholding is required by Applicable Law, Client shall

notify Accenture and will pay any additional amounts necessary to ensure that the net amount that Accenture receives, after any deduction and withholding, equals the amount Accenture would have received if no deduction or withholding had been required. Additionally, Client will provide Accenture with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

- 5.3 Client shall be responsible for the payment of all taxes in connection with the Cloud Agreement including, but not limited to, sales, use, excise, value-added, business, service, goods and services, consumption, withholding, and other similar taxes or duties, including taxes incurred on transactions between and among Accenture, its Affiliates, and third party sub-contractors. Client will reimburse Accenture for any deficiency relating to taxes that are Client's responsibility under the Cloud Agreement. Each Party will be responsible for its own income taxes, employment taxes, and property taxes. The Parties will cooperate in good faith to minimize taxes to the extent legally permissible. Each Party will provide to the other Party any resale exemption, multiple points of use certificates, treaty certification and other exemption information reasonably requested by the other Party.
- 5.4 All amounts payable under the Cloud Agreement will be made without set-off or counterclaim, and without any deduction or withholding.

## 6 INTELLECTUAL PROPERTY RIGHTS

- 6.1 Accenture and the Cloud Vendor(s) (and their third party licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to (i) the systems, software and other content and materials used in the provision of the Cloud Services; and (ii) any suggestions, ideas, enhancement requests, feedback or recommendations provided by Client or any other party relating to the Cloud Services, and Client hereby assigns any Intellectual Property Rights in such items to Accenture. The Accenture name, the Accenture logo, and the product names associated with the Cloud Services are trademarks of Accenture or third parties, and no right or license is granted to Client to use them.

## 7 WARRANTIES AND EXCLUSIONS

- 7.1 Accenture warrants that the Cloud Services provided to Client pursuant to the Cloud Agreement will comply in all material respects with the Services Descriptions included in the applicable Service Order.
- 7.2 Exclusions. The warranties in the Cloud Agreement shall not apply where; (i) any problems have been caused by accident, abuse or where Client's or Users' access or use of the Cloud Services is not in accordance with the Cloud Agreement or Accenture's instructions, including failure to meet minimum system requirements; (ii) the Cloud Services or any systems, software or other content or materials embodied therein are modified or altered by any party other than Accenture; or (iii) the Cloud Services are provided free of charge, or as a trial, pre-release or beta release.
- 7.3 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED IN SECTION 7.1, ACCENTURE, ITS AFFILIATES AND ITS LICENSORS (INCLUDING ANY CLOUD VENDORS) MAKE NO REPRESENTATIONS AND PROVIDE NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE CLOUD SERVICES OR ANY THIRD PARTY COMPONENTS OR CONTENT EMBODIED THEREIN, INCLUDING ANY WARRANTY THAT THE CLOUD SERVICES WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING CLIENT DATA OR THIRD PARTY COMPONENTS OR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. FURTHERMORE, ACCENTURE, ITS AFFILIATES AND ITS LICENSORS (INCLUDING ANY CLOUD VENDORS) MAKE NO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, OR ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE. THE CLOUD AGREEMENT SETS OUT THE FULL EXTENT OF THE PARTIES' OBLIGATIONS AND LIABILITIES ARISING OUT OF OR IN CONNECTION WITH ANY CLOUD AGREEMENT, AND THERE ARE NO CONDITIONS, WARRANTIES, REPRESENTATIONS OR TERMS, EXPRESS OR IMPLIED, THAT ARE BINDING ON THE PARTIES EXCEPT AS SPECIFICALLY STATED IN THE CLOUD AGREEMENT. TO THE EXTENT PERMITTED BY APPLICABLE LAW, ANY CONDITION, WARRANTY, REPRESENTATION OR TERM WHICH MIGHT OTHERWISE BE IMPLIED INTO OR INCORPORATED IN THE CLOUD AGREEMENT, WHETHER BY STATUTE, COMMON LAW OR OTHERWISE, IS HEREBY EXPRESSLY EXCLUDED.

## 8 THIRD PARTY CLAIMS

- 8.1 Subject to the limitations in Section 9, Accenture will defend (at its sole expense) Client and Client's Affiliates against any claims brought against Client by any third party alleging that Client's use of the Cloud Services, in accordance with the Cloud Agreement, constitutes a direct infringement of a patent enforceable in the United Kingdom issued as of the applicable Service Order Effective Date, copyright, or trade secret of any third party

("Infringement Claim"). In addition to defending at its sole expense, Accenture will be obliged to pay only the amount of any damages finally awarded against Client or the amount of any settlement agreed by Accenture.

- 8.2 Accenture will have no obligations or liability under Section 8.1 for any claims arising from:
- (a) Client Data;
  - (b) Client's or any User's use of the Cloud Services after Accenture has notified Client to discontinue use and Client has been afforded a reasonable opportunity to discontinue such use;
  - (c) any unauthorized modification or use of the Cloud Services;
  - (d) any use of the Cloud Services, or any other act or omission, by Client or a User, that is in breach of the Cloud Agreement;
  - (e) any combination(s) of the Cloud Services with any other product, service, software, content, data or method not supplied by Accenture; or
  - (f) a free (no fee), or trial, pre-release or beta release access to the Cloud Services.
- 8.3 If any portion of the Cloud Services is subject to an Infringement Claim, Accenture may choose (at its election and expense) to: (a) procure the rights to use the alleged infringing portion; (b) replace the alleged infringing portion with a non-infringing equivalent; or (c) modify the alleged infringing portion to make it non-infringing while still providing substantially the same level of functionality. If Accenture determines the actions in Section 8.3 (a) to (c) are not commercially reasonable, Accenture may immediately terminate Client's access to the Cloud Service(s) affected by the alleged infringement.
- 8.4 Subject to the limitations in Section 9, Client shall defend (at its sole expense) Accenture, its Affiliates and licensors against claims brought against Accenture by any third party arising from or related to (i) any use of Cloud Services by Client or Users in violation of Applicable Law; (ii) any allegation that the Client Data violates, infringes or misappropriates the rights of a third party; or (iii) Client's or Users' use of the Cloud Services or other act or omission in violation of the Cloud Agreement ("Unacceptable Use Claim"). The foregoing shall apply regardless of whether the Unacceptable Use Claim arises from the conduct of Client, Users or a third party. In addition to defending at its sole expense, Client will be obliged to pay only the amount of damages finally awarded against Accenture or the amount of any settlement agreed by Client.
- 8.5 Client will have no obligations or liability under Section 8.4 for any claims arising from:
- (a) the Client Data after Client has notified Accenture to delete the Client Data within Accenture's control from the Cloud Services and Accenture has been afforded a reasonable opportunity to do so; and
  - (b) any unauthorized access or use of the Client Data by Accenture that is in breach of the Cloud Agreement, where the violation, infringement or misappropriation would not have occurred but for such breach.
- 8.6 In connection with any Infringement Claims and Unacceptable Use Claims pursuant to Sections 8.1 and 8.4 respectively, the indemnified Party will (a) give the indemnifying Party prompt written notice of the claim; (b) reasonably cooperate with the indemnifying Party (at the indemnifying Party's expense) in connection with the defense and settlement of such claim; and (c) grant the indemnifying Party sole control of the defense and settlement of the claim, except that the indemnifying Party may not consent to the entry of any judgment or enter into any settlement with respect to the claim without the indemnified Party's prior written consent unless the settlement or judgment is purely financial, is paid entirely by the indemnifying Party, is confidential, does not require the indemnified Party to admit to any fault of wrongdoing, and fully releases the indemnified Party from any and all further claims or causes of action relating to the subject matter of the claim. The indemnified Party may, at its expense, participate in the defense and settlement of the claim with counsel of its own choosing. If the indemnifying Party fails to assume control within thirty (30) days of written notice of the claim, the indemnified Party may assume control of the defense of the claim.
- 8.7 **Exclusive Remedy.** SECTION 8.1 CONSTITUTES CLIENT'S SOLE AND EXCLUSIVE REMEDY AND ACCENTURE'S (AND ITS AFFILIATES') ENTIRE LIABILITY TO CLIENT WITH RESPECT TO ANY CLAIM THAT THE CLOUD SERVICES INFRINGE ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.



9 LIMITATION OF LIABILITY

- 9.1 For each Cloud Agreement, each Party's maximum, aggregate liability to the other is limited to direct damages finally awarded in an amount not exceeding the amount(s) Client was required to pay for the applicable Cloud Services during the term of the Cloud Agreement, subject to the following:
- 9.2 For Cloud Services, Accenture's maximum liability to Client for any incident giving rise to a claim will not exceed the amount that Client has paid for those Cloud Services having caused the claim during the 12 months before the incident; provided that in no event will Accenture's aggregate liability for any and all claims relating to the Cloud Services exceed the total amount paid for the same Cloud Services during the term of the Cloud Agreement.
- 9.3 Exceptions. THE LIMITS OF LIABILITY IN THIS SECTION APPLY TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, BUT DO NOT APPLY TO: (I) THE PARTIES' OBLIGATIONS UNDER SECTION 8; (II) VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (III) DAMAGES RESULTING FROM DEATH OR BODILY INJURY ARISING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OR FROM FRAUDULENT MISREPRESENTATION; AND (VI) ACCENTURE'S RIGHT TO COLLECT UNPAID FEES DUE HEREUNDER, UNDER NO CIRCUMSTANCES AND REGARDLESS OF THE NATURE OF ANY CLAIM SHALL EITHER PARTY (OR THEIR RESPECTIVE AFFILIATES OR ACCENTURE'S LICENSORS) BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY UNDER THE CLOUD AGREEMENT FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID FOR THE APPLICABLE CLOUD SERVICE UNDER THE SERVICE ORDER THAT GAVE RISE TO THE LIABILITY IN THE TWELVE (12) MONTH PERIOD PRECEDING THE DATE OF THE INCIDENT GIVING RISE TO LIABILITY.
- 9.4 Exclusions. TO THE EXTENT PERMITTED BY APPLICABLE LAW NEITHER PARTY NOR ANY OF EITHER PARTY'S RESPECTIVE AFFILIATES WILL BE LIABLE TO THE OTHER PARTY, HOWEVER CAUSED OR ON ANY THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES; LOSS OF USE, BUSINESS INTERRUPTION, LOSS OF PROFITS OR SAVINGS, LOSS OF BUSINESS INFORMATION, REVENUES, REPUTATION HARM, OR GOODWILL; UNAVAILABILITY OF ANY OR ALL OF THE CLOUD SERVICES (WITHOUT PREJUDICE TO CLIENT'S RIGHT TO RECEIVE SERVICE CREDITS UNDER A SERVICE ORDER, IF APPLICABLE); INVESTMENTS, DIMINUTION IN STOCK PRICE, EXPENDITURES OR COMMITMENTS RELATED TO USE OF OR ACCESS TO THE CLOUD SERVICES; COST OF PROCUREMENT OF SUBSTITUTE SERVICES; UNAUTHORIZED ACCESS TO, COMPROMISE, ALTERATION OR LOSS OF CLIENT DATA; OR COST OF REPLACEMENT OR RESTORATION OF ANY LOST OR ALTERED CLIENT DATA.
- 9.5 The Parties acknowledge that the limitations on liability set out in this Section 9 are essential terms of the Cloud Agreement and the Parties would not have entered the Cloud Agreement without them.
- 9.6 To the extent permitted by Applicable Law, no action, regardless of form, arising out of the Cloud Agreement may be brought by Client more than two (2) years after Client knew or should have known of the event which gave rise to the cause of action.

10 TERM AND TERMINATION

- 10.1 The term of the Cloud Service Terms will commence on the Cloud Terms Effective Date and will continue until terminated by either Party pursuant to this Section 10 ("Term"). The term of any Service Order shall be agreed in the Service Order itself, and the terms and conditions of the Cloud Service Terms shall survive and remain in force to govern any Service Order the term of which exceeds any termination of the Cloud Service Terms.
- 10.2 Either Party may terminate the Cloud Service Terms for convenience upon ninety (90) days' written notice to the other Party.
- 10.3 Either Party may terminate the Cloud Service Terms or any Service Order with immediate effect upon written notice if the other Party ceases its business operations or becomes subject to insolvency proceedings, and the proceedings are not dismissed within ninety (90) days, or otherwise becomes generally unable to meet its obligations under the Cloud Service Terms or the Service Order.
- 10.4 In addition to any other remedies that a Party may have at law, in equity, or under the Cloud Service Terms, a Party may terminate the Cloud Service Terms and/or the relevant Service Order upon [thirty (30)] days' written notice to the other Party if the other Party commits any material breach of the Cloud Service Terms and/or the relevant Service Order, and fails to cure such material breach (if curable) within the [thirty (30)] day period,

including if there has been any such act or omission by Client or any User that has given Accenture the right to suspend the provision of Cloud Services in accordance with Section 2.2.

- 10.5 Accenture may terminate the Cloud Service Terms and/or the relevant Service Order upon [thirty (30)] days' written notice to Client (i) in the event where the underlying contract between Accenture and the Cloud Vendor concerning the provision of Cloud Vendor Solution terminates, or (ii) if termination of the Cloud Service Terms and/or the relevant Service Order is necessary to comply with Applicable Law or binding requests of governmental entities with an authority make such request.
- 10.6 Upon the effective date of expiration or termination of a Service Order, Accenture shall immediately cease Client's and Users' access to and use of the Cloud Services governed by such Service Order.
- 10.7 Client shall have the ability to access and extract Client Data for a period of ninety (90) days after the expiration or termination of the applicable Service Order ("Retention Period"). Accenture will procure that the applicable Cloud Vendor will retain the Client Data for the Retention Period, during which Client will cover the costs of the data storage unless otherwise agreed in the Service Order. After the Retention Period, all Client Data will be deleted.
- 10.8 If mutually agreed by the Parties in a Service Order, Accenture shall provide to Client reasonable co-operation and assistance to facilitate the orderly wind down of the usage of the Cloud Services and/or to assist Client to transition to another service provider. Client will pay Accenture for such assistance at Accenture's then-current time and materials rates for the applicable services or as otherwise mutually agreed by the Parties.

## 11 CONFIDENTIALITY

- 11.1 Except as set forth in Section 11.2, each Party shall (i) not disclose, publish or communicate the other Party's Confidential Information to any third party, and (ii) use and disclose the other Party's Confidential Information only for purposes of the Parties' business relationship with each other as contemplated by the Cloud Agreement. Each Party agrees to take reasonable steps to protect the other's Confidential Information, provided that these steps must be at least as protective as those the Party takes to protect its own Confidential Information of similar nature, but in any event no less than a reasonable standard of care.
- 11.2 Each Party may disclose the other Party's Confidential Information to its Affiliates, employees, contractors, licensors and agents who: (i) have a need to know it for purposes contemplated by the Cloud Agreement, and (ii) are legally bound to protect the Confidential Information on terms no less protective than the terms of the Cloud Agreement.
- 11.3 This Section 11 will not apply to any information that either Party can demonstrate: (i) was at the time of disclosure or that has become thereafter published or otherwise becomes part of the public domain through no fault of the receiving Party; (ii) was in the possession of the receiving Party at the time of disclosure to it and was not the subject of a pre-existing confidentiality obligation; (iii) was received after disclosure to it from a third party who had a lawful right to disclose such information (without corresponding confidentiality obligations) to it; or (iv) was independently developed by the receiving Party without use of the Confidential Information of the disclosing Party.
- 11.4 The receiving Party will not be considered to have breached its obligations under this Section 11 for disclosing Confidential Information of the disclosing Party to the extent required to satisfy any legal requirement of a competent governmental or regulatory authority, provided that promptly upon receiving any such request and to the extent that it may legally do so, the receiving Party: (i) advises the disclosing Party prior to making such disclosure so that the disclosing Party may object to such disclosure or take any other action that it considers appropriate to protect the Confidential Information and; (ii) takes actions necessary to minimize any disclosure to only that necessary to satisfy the legal requirement (including through redaction of sensitive commercial information, where legally permissible).
- 11.5 Any reproduction of any Confidential Information of the other Party shall remain the property of the disclosing Party, and the disclosing Party may, at any time including on termination of the Cloud Agreement, request the receiving Party to return, destroy or delete (and confirm the destruction or deletion of the same) as instructed (in such a manner that it cannot be recovered) all Confidential Information of the disclosing Party in the receiving Party's possession or control. Notwithstanding the foregoing, each Party may archive all copies of Confidential Information that it is required to retain to comply with law and its other record-keeping requirements.
- 11.6 Client shall not disclose the terms and conditions of the Cloud Agreement or the pricing contained therein to any third party without the prior written consent of Accenture. Neither Party shall use the name of the other Party in publicity, advertising, or similar activity, without the prior written consent of the other Party. Notwithstanding the aforesaid, Client acknowledges and agrees that Accenture may provide information regarding Client's purchase,

use and consumption of Cloud Vendor Solution, and the related terms, to the relevant Cloud Vendor, subject to obligations of confidentiality with the Cloud Vendor.

## 12 ADDITIONAL TERMS

- 12.1 Compliance with Export Control Laws. Each Party will comply with all export control and economic sanctions laws applicable to its performance under the Cloud Agreement. Client agrees that Client will not, and will procure that Users do not, use the Cloud Services in or in relation to any activities involving a country subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria or the Crimea region of Ukraine), or involving a party in violation of such applicable trade control laws, or that require government authorization, without first obtaining the written consent of Accenture and the required authorization. For the avoidance of doubt, Client shall not grant access to the Cloud Services to any individual, entity or organization that is subject to trade sanctions or embargos by the United States, or to any applicable jurisdiction, individual, entity or organization that is listed on the OFAC Specially Designated Nationals List from time to time.
- 12.2 Notices. Unless expressly stated otherwise in the Cloud Agreement, all notices under the Cloud Agreement must be (i) in writing, (ii) in the English language and (iii) delivered personally, sent by certified mail (return receipt requested) or sent by express courier (with confirmation of delivery). The notice will be deemed given and will be effective: (a) upon receipt when it is delivered to a Party personally; (b) upon receipt if sent through certified mail, return receipt requested; or (c) upon delivery by a nationally recognized overnight courier service such as FedEx (with confirmation of delivery). All notices must be addressed to the other Party at the address set forth herein, plus Client must also send a copy of its notice (except for routine correspondence) to: Accenture LLP, Legal – General Counsel, 161 North Clark Street, Chicago, Illinois 60601. Either Party may designate a different address by giving ten (10) days' written notice to the other Party.
- 12.3 Governing Law and Jurisdiction. The laws of [*the State of Illinois and federal laws of the United States*] will govern the construction, validity and operation of the Cloud Agreement and the performance of all obligations hereunder without regard for Illinois' choice of law provisions. The courts of [*Chicago, Illinois*] shall have exclusive jurisdiction in relation to any dispute or matter arising under or in connection with the Cloud Agreement.
- 12.4 Force Majeure. Other than Client's obligation to pay Accenture pursuant to the Cloud Agreement, neither Party will be liable for any delay or failure to perform any obligation under the Cloud Agreement due to causes beyond that Party's reasonable control, including without limitation electrical or power outage, utilities or telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war, or labour disputes with its or its Affiliates' employees, or industrial disturbances.
- 12.5 Survival. The provisions of Sections 5, 6, 9, 10, 11 and 12, and any other Sections that by their nature are intended to survive, will survive the termination of the Cloud Agreement.
- 12.6 Assignment. Client may not assign the Cloud Agreement or delegate or sublicense any of Client's rights or obligations hereunder, including by operation of law, without the prior written consent of Accenture and any attempt to do so in violation of this provision will be null and void. The Cloud Agreement will be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns. Accenture may assign or subcontract all or part of its obligations under the Cloud Agreement to Accenture Affiliates or sub-contract the same to any Cloud Vendor(s) (who may in turn subcontract all or part of its obligations to third parties).
- 12.7 Variation. The Cloud Agreement may not be modified or amended except by the mutual written agreement of the authorized representatives of the Parties.
- 12.8 No waiver. No waiver of any provision of the Cloud Agreement will be effective unless it is in writing and signed by the Party against which it is sought to be enforced. The delay or failure by either Party to exercise or enforce any of its rights under the Cloud Agreement is not a waiver of that Party's right to later enforce those rights, nor will any single or partial exercise of any right preclude any other or further exercise of these rights or any other right.
- 12.9 Severability. If a court of competent jurisdiction finds any term of the Cloud Agreement to be invalid, illegal or otherwise unenforceable, such term will not affect the other terms of the Cloud Agreement. Such term will be deemed modified to the extent necessary, in the court's opinion, to render such term enforceable while preserving to the fullest extent possible the intent and agreements of the Parties set forth in the Cloud Agreement. To the extent permitted by law, the Parties agree that any principle of construction or rule of law that provides that an agreement will be construed against the drafter will not apply to the Cloud Agreement.
- 12.10 Entire Agreement. The Cloud Agreement, together with any appendices, attachments, exhibits or referenced documents contain the entire agreement between the Parties with respect to the Cloud Services and supersedes all prior agreements, conditions, warranties, representations, arrangements and communications, whether written or verbal, and whether with or by Accenture, any of its Affiliates, or any of their employees, officers, directors,

agents or shareholders regarding the subject matter of the Cloud Agreement. Each Party acknowledges that it is entering into the Cloud Agreement solely on the basis of the agreements and representations contained herein, and that it has not relied upon any representations, warranties, promises, or inducements of any kind, whether oral or written, and from any source.

- 12.11 Relationship of the Parties. Nothing in the Cloud Agreement will be deemed to create a joint venture, partnership, or agency relationship between the Parties or be deemed to authorize either Party to incur any liabilities or obligations on behalf of, or in the name of, the other. Accenture and Client are independent contractors.
- 12.12 Third Party Rights. Accenture's licensors are third party beneficiaries hereunder. The Cloud Agreement does not otherwise create any third-party beneficiary rights, and in particular it is agreed that Client's Users are not third-party beneficiaries.
- 12.13 Counterparts. The Cloud Service Terms and any Service Order may be executed electronically and in multiple counterparts, each of which will be considered an original, and all of which together will constitute one agreement binding on the Parties, even if both Parties are not signatories to the original or same counterpart.

## Appendix A – Definitions

**“Affiliate”** of a Party means any entity, whether incorporated or not, that is Controlled by, Controls, or is under common Control with such Party. “Control” means the ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise;

**“Applicable Law(s)”** means any federal, state, provincial, local, municipal, regional, foreign, international, multinational or other constitution, law, statute, treaty, rule, regulation, regulatory or legislative requirement, ordinance, code, common law or other pronouncement having the effect of law;

**“Client Data”** means any content, materials, data and information that Client or Users enter into a Cloud Services or Client-specific data that is derived from Client’s use of the Cloud Services (e.g. Client-specific reports), as long as such output data is not a component of the Cloud Services itself or furnished by Accenture under the Agreement. Client Data shall not include any component of the Cloud Services or material provided by or on behalf of Accenture;

**“Cloud Agreement”** shall have the meaning set out in Section 1.1;

**“Cloud Service(s)”** means [the cloud based services further described in the applicable Service Order(s)];

**“Cloud Service Terms”** shall have the meaning set out in Section 1.1;

**“Cloud Service Terms Effective Date”** means the date on which the Cloud Service Terms was entered in to;

**“Cloud Vendor”** means a third-party cloud service provider, providing a Cloud Vendor Solution, as identified in the relevant Service Order;

**“Cloud Vendor Solutions”** means a cloud service identified in a relevant Service Order that is provided by a Cloud Vendor and that forms a component of the Cloud Services provided by Accenture;

**“Confidential Information”** means information that relates to the other Party’s (or to Cloud Vendor’s) past, present, or future research, development, business activities, products, services, and technical knowledge, which is identified by the discloser as confidential or that would be understood to be confidential by a reasonable person under the circumstances;

**“Fees”** means the fees specified in the relevant Service Order and payable in accordance with Section 5 or the relevant Service Order;

**“High Risk Activities”** means usage such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems environments where the use or failure of the Service could lead to death, personal injury or environmental damage;

**“Intellectual Property Rights”** means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights, derivatives thereof, and forms of protection of a similar nature;

**“Party”** or **“Parties”** means Accenture and/or Client;

**“Personal Data”** means data which names or identifies a natural person including, without limitation: (a) data that is explicitly defined as a regulated category of data under data privacy laws applicable to Client; (b) non-public personal data, such as national identification number, passport number, social security number, driver’s license number; (c) health or medical information, such as insurance information, medical prognosis, diagnosis information or genetic information; (d) financial information; and/or (e) sensitive personal data, such as race, religion, marital status, disability, or sexuality;

**“Service Order Effective Date”** means the date on which the Service Order was entered in to;

**“User”** means any individual or entity that the Parties agree in a Service Order may access or use the Cloud Services, or access or use the Client Data; and

**“Virus”** means any item, software, device or code which is intended by any person to, or which is likely to, or which may:

- (a) impair the operation of any software or computer systems;
- (b) cause loss of, or corruption or damage to any software or computer systems or data;
- (c) prevent access to or allow unauthorised access to any software or computer system or data; and / or
- (d) damage the reputation of Client and / or Accenture,

including any computer virus, Trojan horse, worm, software bomb, authorization key, license control utility or software lock.

# Service Order

## [AMAZON WEB SERVICES (AWS)]

1. **Acceptable Use Policy.** Client acknowledges that its access and use of the Platform Services (including IaaS) shall be subject to the Cloud Vendor's Acceptable Use Policy <https://aws.amazon.com/aup/> as updated by the Cloud Vendor from time to time. Client agrees that it is solely responsible for monitoring any changes to the Acceptable Use Policy and for ensuring that its own, its Affiliates', and its and its Affiliates' Authorized Users' access and use of the IaaS shall comply with the said policy. Client acknowledges and accepts that any violation of the Acceptable Use Policy may lead to suspension of the Platform Services in accordance with Sections 3.6 and 3.7 of the Agreement.
2. **Service Terms.** *[Client acknowledges that its access and use of the Platform Services shall be subject to the Cloud Vendor's:*  
  
*"Terms of Use" means the terms of use located at <http://aws.amazon.com/terms/>, as they may be updated by Cloud Vendor from time to time.*  
  
*"Service Terms" means the rights and restrictions for **particular Cloud Services** located at <http://aws.amazon.com/serviceterms>, as they may be updated by Cloud Vendor from time to time. ]*
3. **Service Level Agreement.** The Cloud Vendor shall provide the IaaS in accordance with the applicable Service Level Agreement which can be located at: <http://aws.amazon.com/ec2-sla/> / <http://aws.amazon.com/s3-sla/> / <http://aws.amazon.com/cloudfront/sla/> / <http://aws.amazon.com/route53/sla/>. Client acknowledges that the Cloud Vendor has reserved the right to make changes to, replace and discontinue the applicable Service Level Agreement from time to time, but where such change will materially reduce the benefits offered to Client under the Service Level Agreements in relation to the IaaS, it will only apply to Client sixty (60) days after the effective date of that change.
4. **Security.** The Cloud Vendor shall provide the IaaS in accordance with the Cloud Vendor Security Standards attached hereto as **Attachment A**, subject to Accenture and Client complying with the Encryption and Security Architecture Requirements attached hereto as **Attachment B**. Client acknowledges that the Cloud Vendor has reserved the right to modify the Cloud Vendor Security Standards from time to time, provided that it continues to provide at least the same level of security as described in the Cloud Vendor Security Standards.
5. **[Security Audit Reports.** *Cloud Vendor uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which Cloud Vendor provides the IaaS. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at Cloud Vendor's selection and expense; and (d) will result into a confidential summary concerning the results of the audit ("Summary Report") so that Client can reasonably verify Cloud Vendor's compliance with the security obligations under this Schedule 1. At Client's written request to Accenture, and provided that Client has first executed Cloud Vendor's standard unilateral non-disclosure agreement, Accenture will procure from Cloud Vendor a copy of the confidential Summary Report for Client.]*
6. **Hosting of Client Data.** Client may specify the location(s) where Client Data will be hosted, including the EU (Dublin) Region, the EU (Frankfurt) Region, the US East (Northern Virginia) Region, the US West (Northern California) Region, the US West (Oregon) Region, the South America (Sao Paulo) Region, the Asia Pacific (Tokyo) Region, the Asia Pacific (Singapore) Region and the Asia Pacific (Sydney) Region (each a "**Region**"). Once Client has made its choice, Cloud Vendor will not transfer Client Data from Client's selected Region(s) without first notifying the Client, unless necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order).
7. **Processing of Client Data.** Accenture has entered into an agreement with Cloud Vendor that incorporates the EU Standard Contractual Clauses, as per European Commission Decision of 5 February 2010, for the transfer of personal data outside of the EU. The EU Standard Contractual Clauses, as published on <http://aws.amazon.com/compliance/eu-data-protection/> (or such other location as may be updated from time to time) form a part of this Exhibit and the Agreement insofar that the Infrastructure Services are concerned, and the Cloud Vendor shall comply with them, whether acting as a data processor or sub-processor. *[Cloud Vendor's personnel will not access, use or disclose Client Data, except as necessary to maintain the IaaS, or retrieve or read any Client Data in human readable form in the ordinary course of providing the IaaS.]*
8. **Security Accreditations.** As of the Effective Date, as to its service offerings, Cloud Vendor (a) is certified compliant with ISO 27001 by an Accredited Registrar, (b) is validated by a QSA as compliant as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS) for specified cloud environments (set out at <http://aws.amazon.com/compliance/>), which require procurement of the appropriate service, including any associated costs, (c) has a FedRAMP authorization from the U.S. Department of Health and Human Services for specified cloud environments (set out at <http://aws.amazon.com/compliance/>), which require procurement of the appropriate service,

including any associated costs, and (d) maintains the controls described in the SOC 1 Report and the SOC 2 Report. Accenture will provide Client at least thirty (30) days' prior notice if, during the Term, Accenture knows that Cloud Vendor will (a) not seek recertification as compliant with ISO 27001 (or a substantially equivalent standard), (b) not seek to be validated as compliant as a Level 1 service provider under the PCI-DSS (or a substantially equivalent standard), (c) not seek to maintain FedRAMP compliance (or substantially equivalent standard) or (d) no longer maintain the controls described in the SOC 1 Report or the SOC 2 Report (or a substantially equivalent standard).

9. **HIPAA Data.** Client warrants and represents that it will not provide any "protected health information" (as defined in 45 CFR 160.103 of the US Health Insurance Portability and Accountability Act) to Accenture in connection with Client's access to and use of the Platform Services. If Client wishes to provide any such protected health information in connection with the Platform Services, Client shall contact Accenture to request this and the terms related to the provision of a HIPAA account.



# Attachment A

## Security Standards

**[DRAFTING NOTE: To be reviewed in the context of the engagement.]**

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable Attachment [X].

1. **Information Security Program.** Cloud Vendor will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Cloud Vendor Network, and (c) minimize security risks, including through risk assessment and regular testing. Cloud Vendor will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:
2. **Network Security.** The Cloud Vendor Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Cloud Services. Cloud Vendor will maintain access controls and policies to manage what access is allowed to the Cloud Vendor Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Cloud Vendor will maintain corrective action and incidence response plans to respond to potential security threats.
3. **Physical Security**
  - a. **Physical Access Controls.** Physical components of the Cloud Vendor Network are housed in nondescript facilities (the “Facilities”). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.
  - b. **Limited Employee and Contractor Access.** Cloud Vendor provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Cloud Vendor or its affiliates.
  - c. **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Cloud Vendor also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.
  - d. **Pre-Employment Screening.** Cloud Vendor conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees and contractors commensurate with the employee’s or contractor’s position and level of access to the Facilities. Cloud Vendor will not permit an employee or contractor to have access to the non-public Client Content or perform material aspects of the Cloud Services if such employee or contractor has failed to pass such background check.
4. **Continued Evaluation.** Cloud Vendor will conduct periodic reviews of the security of the Cloud Vendor Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Cloud Vendor will continually evaluate the security of the Cloud Vendor Network and associated Cloud Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.
5. **Security Breach Notification.** Accenture will notify Client of a breach of security if and to the extent required by security breach notification laws applicable to Accenture, and will take commercially reasonable measures to address the breach in a timely manner. The term “breach of security” means the unauthorized access to or acquisition of any record containing Client Content in a manner that renders misuse of the information reasonably possible. Accenture’s obligation to report or respond to a security breach is not to be construed as an admission by Accenture of any fault or liability with respect to the security breach.



## Attachment B

# Encryption and Security Architecture Requirements

At all times Client will comply with the following encryption requirements (the “**Encryption Requirements**”):

1. Client will encrypt all Client Content in transit by using SSL/TLS or other industry-standard encryption mechanisms.
2. Client will protect Client Content at rest as follows:
  - a. At all times Client Content at rest will be encrypted using industry-standard encryption mechanisms.
  - b. Client will implement cryptographic key management procedures sufficient to appropriately secure key material.
  - c. Unencrypted Client Content will not be utilized as metadata or as parameters for configuring Cloud Services.
  - d. Unencrypted Client Content will not be stored as part of an Amazon Machine Image (“**AMI**”).
  - e. Client will not store account credentials as part of an AMI.

At all times Client will comply with the following security architecture requirements (the “**Security Architecture Requirements**”):

1. Client will utilize all published security best practices in the Security Best Practices document available at <http://aws.amazon.com/security/security-resources/>. Client will comply with any updates or changes to the security best practices described above as soon as reasonably practicable (and in any event not later than sixty (60) days) following such update or change.
2. For all Cloud Services processing Client Content, Client will use Amazon Virtual Private Cloud when available.
3. Client will not use root account credentials beyond initial account configuration of Cloud Vendor Identity and Access Management (“**IAM**”), except for Cloud Services for which IAM is not available.
4. Client will manage multiple Users (as described on the Cloud Vendor Site) and their permissions with IAM or Security Token Service as follows:
  - a. Use the principle of least privilege.
  - b. The privileges granted to Users, Groups, and Secure Tokens (each as described on the Cloud Vendor Site) will be no more than the minimal privileges necessary.
  - c. Every User will have unique security credentials.
  - d. All security credentials will be regularly rotated, no less than quarterly.
  - e. All Cloud Vendor Management Console authentications will be via IAM Users using multifactor authentication or utilizing federated credentials.
5. Access limitation: Client will minimize permissions in Security Groups (as described on the Cloud Vendor Site) and Access Control Lists (as described on the Cloud Vendor Site) only to those users required for the operation of Client’s services. Client will minimize source and destination authorizations permitted to solely those required for the operation of Client’s services.

# Service Order

## [MICROSOFT AZURE (AZURE)]

1. **Order of Precedence.** These Azure Specific Terms complement the Cloud Service Terms and form a part of the Cloud Agreement. These Azure Specific Terms govern the provision and consumption of Azure Services alone (as defined below). In the event of any conflict or inconsistency between these Azure Specific Terms and the Cloud Service Terms, these Azure Specific Terms shall prevail to the extent of the conflict or inconsistency.
2. **Definitions.**

“**Azure Services**” means the Microsoft services and features identified at <http://azure.microsoft.com/services/>, except those licensed separately. “Azure Services” includes any open source components incorporated by Microsoft in those services and features.

“**Online Services Terms**” means the additional terms that will apply to Client’s use of Azure Services, published at <https://www.microsoft.com/en-gb/Licensing/product-licensing/products.aspx> and updated by Microsoft from time to time.

“**Acceptable Use Policy**” is set forth in the Online Services Terms.

“**Service Level Agreement**” or “**SLA**” means the relevant service level agreement applicable to the Azure Services that Client has subscribed to, published at <https://www.microsoft.com/en-gb/Licensing/product-licensing/products.aspx> and updated by Microsoft from time to time.
3. **Online Service Terms.** Client agrees that the provision of Azure Services, and the Client’s access and use of the Azure Services is Microsoft’s Online Service Terms. Client agrees that the Online Service Terms form a binding and enforceable part of the Cloud Agreement, as far as Azure Services are concerned, and they will govern to the Azure Services that Client has subscribed to. The Online Services Terms in effect when Client orders a new, or renews an existing subscription will apply to the Azure Services in question, for the applicable subscription term. For Azure Services that are billed periodically based on consumption, the Online Services Terms current at the start of each billing period will apply to usage during that period. Accenture recommends that Client downloads and prints out the Online Service Terms for Azure Services in full for future reference.
4. **Acceptable Use Policy.** Client acknowledges and agrees that its access and use of the Azure Services shall be subject to the Cloud Vendor’s Acceptable Use Policy which is incorporated in the above-mentioned Online Service Terms. Client agrees that it is solely responsible for ensuring that its own, its Affiliates and its Users access and use of the Azure Services shall comply with this policy. Client acknowledges and accepts that any violation of the Acceptable Use Policy may lead to suspension of the Azure Services in accordance with the Cloud Services Terms [Sections 2.8 and 2.9].
5. **Service Level Agreement.** Microsoft shall provide the Azure Services in accordance with the relevant Service Level Agreement applicable to the Azure Services that Client has subscribed to. Client agrees that the Service Level Agreement for Azure Services will form a part of the Cloud Agreement as far as the Azure Services are concerned. Accenture recommends that Client downloads and prints out the Service Level Agreement for Azure Services in full for future reference.
6. **Limited Warranty.** Microsoft has warranted to Accenture that each Azure Service will perform in accordance with the applicable SLA during Client’s use. Client’s remedies for breach of this warranty are in the SLA. Microsoft has further warranted to Accenture that during the term of each Subscription for an Azure Service, it will provide the Azure Service as described in the Online Service Terms. The remedies above are Client’s sole remedies for breach of the warranties in this section. Client waives any breach of warranty claims not made during the warranty period. The aforesaid warranties do not apply to free or trial products, previews and limited offerings. Furthermore, for Azure Services provided free of charge, Accenture’s liability is limited to direct damages finally awarded up to US\$5,000.
7. **Compliance and Certifications.** Microsoft’s existing compliance certifications for Azure Services can be found in the Online Service Terms and the most current certifications have been listed at <http://azure.microsoft.com/en-us/support/trust-center/>. For the avoidance of doubt, nothing in this paragraph shall apply to or modify Accenture’s obligations with respect to any data processing or security provisions agreed between Accenture and Client.
8. **General Privacy and Security Terms.** Azure Services shall be subject to the General Privacy and Security Terms included in the Online Service Terms. Client acknowledges and agrees that (i) Accenture will be the primary administrator of the Azure Services for the term of the applicable Cloud Agreement, and that Accenture will have administrative privileges and access to Client Data, however, Client may request additional administrator privileges from Accenture; (ii) Client can, at its sole discretion and at any time during the term of the Cloud Agreement, terminate Accenture’s administrative privileges; (iii) Accenture’s privacy practices with respect to Client Data or any services provided by Accenture are subject to the terms of Client’s agreement with Accenture and may differ from

Microsoft's General Privacy and Security Terms included in the Online Service Terms; and (iv) Accenture may collect, use, transfer, disclose, and otherwise process Client Data, including personal data. Client consents to Accenture providing Accenture with Client Data and information that Client provides to Accenture for purposes of ordering, provisioning and administering the Azure Services. Client appoints Accenture as its agent for purposes of interfacing with and providing instructions to Accenture for purposes of this Section 8. The commitments made in the Online Services Terms only apply to the Azure Services purchased under the Cloud Agreement, and not to any other services or products provided by a Accenture. If Client uses software or services that are hosted by Accenture, that use will be subject to Accenture's privacy practices, which may differ from Microsoft's.

9. **Subprocessors.** Client acknowledges and accepts that Microsoft may hire third parties to provide certain limited or ancillary services on its behalf. Customer consents to the engagement of these third parties and Microsoft Affiliates as subprocessors. The above authorizations will constitute Client's prior written consent to the subcontracting by Microsoft of the processing of Client Data and any personal data contained therein, if such consent is required under the Standard Contractual Clauses or the GDPR Terms. Additional terms concerning such subprocessors are in the Online Services Terms. Further details regarding who can access Client Data hosted and processed on Azure Services is provided at <https://www.microsoft.com/en-us/trustcenter/Privacy/Who-can-access-your-data-and-on-what-terms>

**[THE FOLLOWING PROVISIONS CAN BE EITHER INCLUDED OR REMOVED DEPENDING ON WHETHER THEY ARE APPLICABLE]**

**Support.** Accenture will provide details on support services available for Products purchased under this agreement. Support services may be performed by Accenture or its designee, which in some cases may be Microsoft.

**Preview releases.** Microsoft may make Previews available. Previews are provided "as-is," "with all faults," and "as-available," and are excluded from the SLA and all limited warranties provided in this agreement. Previews may not be covered by Client support. Previews may be subject to reduced or different security, compliance, and privacy commitments, as further explained in the Online Services Terms and any additional notices provided with the Preview. Microsoft may change or discontinue Previews at any time without notice. Microsoft also may choose not to release a Preview into "General Availability."

**Eligibility for Academic, Government and Nonprofit versions.** Client agrees that if it is purchasing an academic, government or nonprofit offer, Client meets the respective eligibility requirements listed at the following sites:

- (i) For academic offers, the requirements for educational institutions (including administrative offices or boards of education, public libraries, or public museums) listed at <http://go.microsoft.com/academic>;
- (ii) For government offers, the requirements listed at <http://go.microsoft.com/government>; and
- (iii) For nonprofit offers, the requirements listed at <http://go.microsoft.com/nonprofit>.

Accenture reserves the right to verify eligibility at any time and suspend the Azure Service if the eligibility requirements are not met.

# Service Order

## [Google Cloud (Google)]

1. **Services.** The Infrastructure Services consist of those applicable [compute, hosting and management functions for the data center and host systems infrastructure] as described [in the Service Order/below/link to vendor's service descriptions]. Client acknowledges that the Cloud Vendor's terms relating to the Infrastructure Services set forth at <https://cloud.google.com/terms/service-terms> ("**Service Specific Terms**", updated by the Cloud Vendor from time to time) shall apply to the Client's use of the Infrastructure Services and Client shall comply with the same.
2. **Acceptable Use Policy.** Client acknowledges that its access and use of the Infrastructure Services shall be subject to the Cloud Vendor's Acceptable Use Policy at <https://cloud.google.com/terms/aup> ("**AUP**") as updated by the Cloud Vendor from time to time. Client agrees that it is solely responsible for monitoring any changes to the AUP and for ensuring that its own, its Affiliates and its End Users access and use of the Infrastructure Services shall comply with the AUP. Client acknowledges and accepts that any violation of the AUP may lead to suspension of the Infrastructure Services in accordance with Sections [2.4-2.6] of the Agreement. Client further agrees that if Cloud Vendor has a good faith belief that Client Data violates the AUP, then in addition to any other rights it or Accenture might have under this Agreement, Cloud Vendor may review such Client Data solely for compliance with the AUP.
3. **Additional Restrictions.** Client agrees that it shall not (and shall ensure that its End Users shall not) (i) use the Infrastructure Services to create, train or improve a substantially similar product or service, including any other machine translation engine; (ii) process or store any Client Data that is subject to the International Traffic in Arms Regulations maintained by the Department of State; or (iii) use the Infrastructure Services to operate or enable any telecommunications service or in connection with any application that allows End Users to place calls or to receive calls from any public switched telephone network.
4. **[Service Level Agreement.** Cloud Vendor shall provide the Infrastructure Services in accordance with the applicable Service Level Agreement [set forth in Attachment A hereto] as updated by the Cloud Vendor from time to time.]
5. **Security.** Cloud Vendor will take and implement the security measures set out at <https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures>. Client acknowledges and accepts that the Cloud Vendor may update or modify such security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Infrastructure Services.
6. **Reviews of Security Documentation.** Upon request Cloud Vendor will make the following available for review by Client:
  - (a) the certificate issued in relation to Google's ISO 27001 Certification;
  - (b) the then-current SOC 3 Report;
  - (c) a summary or redacted version of the then-current confidential SOC 2 Report; and
  - (d) following a request by Customer in accordance with Section 6.5.4 below, the then-current confidential SOC 2 Report.
7. **Location of Client Data.** Except as otherwise agreed in the Service Specific Terms, Cloud Vendor may process and store Client Data in the United States or any other country in which the Cloud Vendor or its agents maintain facilities.
8. **Processing of Client Data.** To the extent that Cloud Vendor processes Client Data which contains personal data (as defined in EU Directive 95/46/EC) under this Agreement, it shall implement and maintain sufficient technical and organisational measures designed to safeguard such personal data (as further detailed at <https://cloud.google.com/security/>). Accenture has further entered into an agreement with Cloud Vendor that incorporates the EU Standard Contractual Clauses, as per European Commission Decision of 5 February 2010, for the transfer of personal data outside of the EEA. Cloud Vendor shall comply with its obligations under such EU Standard Contractual Clauses, whether acting as a data processor or sub-processor.
9. **HIPAA Data.** Client warrants and represents that it will not provide any protected health information (as defined in 45 CFR 160.103 of the US Health Insurance Portability and Accountability Act) to Accenture in connection with this Attachment. If Client wishes to provide any such protected health information in connection with the Cloud Services, Client shall contact Accenture to request this and the terms related to the provision of a HIPAA account.

## Attachment A: Service Levels

The following provisions set out Client's rights in relation to the availability of the Infrastructure Services.

**SLAs**. The following SLAs shall apply to the provision of the Infrastructure Services:

- (a) Google App Engine set forth here: <https://developers.google.com/appengine/sla>;
- (b) Google Cloud Storage set forth here: <https://developers.google.com/storage/sla>;
- (c) Google Prediction API set forth here: <https://developers.google.com/prediction/sla>;
- (d) Google BigQuery Service set forth here: <https://developers.google.com/bigquery/sla>;
- (e) Google Cloud SQL set forth here: <https://developers.google.com/cloud-sql/sla>;
- (f) Google Compute Engine set forth here: <https://developers.google.com/compute/sla>; and
- (g) Google Cloud Datastore set forth here: <https://developers.google.com/datastore/sla>.]

