TERMS AND CONDITIONS

These terms and conditions (and Schedule 1) together with the Statement of Work referencing these terms and conditions (together the "**Agreement**") are entered into as of the start date of the Statement of Work ("**Effective Date**") and are between Avanade UK Limited, a company incorporated under the laws of England and Wales (company number: 4042711) having its registered address at 30 Cannon Street, London, EC4M 6XH ("**Avanade**") the client named in the Statement of Work ("**Client**"). Avanade and Client are referred to herein individually as a "**Party**" and collectively as the "**Parties**".

1. Services and Deliverables.

Avanade will perform for Client services ("**Services**") and provide Deliverables as specified in the written statement of work ("**SOW**") executed by the Parties. "**Deliverables**" means software, documents or other tangible items identified as "Deliverables" in the SOW that Avanade delivers to Client. The Services will be performed by Avanade's and its Affiliates' employees, independent consultants and/or subcontractors ("**Personnel**"), as determined by Avanade. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party, with "**control**" meaning ownership of 50% or more of the voting equity interests, or the power to otherwise direct the affairs of such Party. Each SOW forms a separate and binding contract between the executing parties, and the requirements of one SOW will not apply to the Services or Deliverables provided under another SOW. Avanade may perform the Services remotely subject to the operational principles set out in the SOW.

2. Fees.

2.1 Payment.

Client will pay Avanade the fees set forth in the SOW ("**Fees**") and reimburse Avanade for reasonable expenses incurred in performing the Services. Avanade will invoice Client monthly or as specified in the SOW. Client will pay Avanade all undisputed amounts within 30 calendar days of the invoice date in accordance with payment instructions provided by Avanade. Avanade may charge interest on amounts that are not subject to a good faith dispute that were not paid when due at the lesser of 3% per month or the maximum legal rate.

2.2 Taxes.

Each Party is responsible for taxes on its net income, employment taxes and other claims of its employees, and taxes on property it owns or leases, and for any deficiency (including penalties and interest) on these and other taxes that are its responsibility. The Fees do not include taxes and Client will pay taxes due under this Agreement. Unless otherwise agreed in the SOW, if any Avanade Consultant is required to perform Services outside the location where such Consultant is based, Client will reimburse Avanade for increased tax and administrative costs incurred as a result thereof. Client will reimburse and hold Avanade harmless from any deficiency (including penalties and interest) relating to taxes that are Client's responsibility. The Parties will cooperate in good faith to minimize taxes to the extent legally permissible.

3. Deliverables Acceptance.

Deliverables are deemed accepted 10 calendar days (or other period in the SOW) after delivery unless Client notifies Avanade in writing within such period detailing how the Deliverable fails to materially comply with the SOW requirements.

4. Intellectual Property.

4.1 Rights in Deliverables.

Subject to Client's compliance with this Agreement and the SOW (including full payment of any applicable fee), Avanade grants to Client a perpetual, non-transferable, non-exclusive, fully paid-up right and license to use, copy, modify and prepare derivative works of the Deliverables for Client's internal business purposes only. Client does not obtain any rights in Avanade Pre-Existing IP other than what is provided for the Deliverables in this Section 4.1. Unless otherwise provided in the SOW, all intellectual property rights, including without limitation patents, copyright, know-how, trade secrets and other proprietary rights ("**IP**") in the

Deliverables remain in and/or are assigned to Avanade. Avanade Pre-Existing IP embedded in Deliverables may not be used separately. Client will not reverse engineer, disassemble or decompile, or attempt to discover or recreate the source code to the Deliverables or engage in or permit any use, sublicensing, distribution, or other activity that is not authorized by Avanade.

4.2 Pre-Existing IP.

Each Party (or its licensors, as applicable) shall retain ownership of its IP which existed prior to the Effective Date and IP developed, licensed or acquired by or on behalf of a Party or its licensors during the Term (as defined in Section 10) which is not a Deliverable, in each case including any modifications thereto or derivatives thereof (collectively "**Pre-Existing IP**"). Client does not obtain any rights in Avanade Pre-Existing IP other than what is provided for the Deliverables in Section 4.1.

4.3 Client IP.

Client or its third-party licensors own all right, title and interest, including intellectual property rights, in and to any information, equipment, software, data or other materials, including Client Pre-Existing IP, that Client provides to Avanade under this Agreement ("**Client IP**"). Client will obtain any consents and licenses necessary for Avanade to use the Client IP to perform its obligations under this Agreement, and grants Avanade a non-exclusive, worldwide, royalty-free, fully paid-up license to use, display, modify, and prepare derivative works of Client IP as required for Avanade to perform such obligations.

4.4 Residuals.

Each Party is free to use concepts, techniques and know-how retained in the unaided memories of those involved in the performance or receipt of the Services for any purpose. Avanade 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 Confidential Information.

4.5 Third Party Products.

The rights and terms of use for third party products, including open source, community or other free code or libraries of any type ("**Third Party Products**"), will be governed by the license between Client and such third parties.

5. Confidentiality.

Each Party may have access to information that relates to the other Party's business activities, including research, development, products, services, processes and technical knowledge, which is identified by the disclosing Party as confidential or is reasonably understood to be confidential ("**Confidential Information**"). Each Party will protect the confidentiality of the other Party's Confidential Information in the same manner as it protects its own similar information, but in any event using a reasonable standard of care. Each Party will use the other Party's Confidential Information only as necessary to perform its obligations under this Agreement and will restrict access to such Confidential Information to its and its Affiliates' personnel engaged in the performance, receipt or use of the Services, provided that such personnel are bound by obligations of confidentiality no less protective than under this Agreement. Except for any license or right expressly granted under this Agreement, each Party reserves all right, title and interest in or to its Confidential Information. The Parties' obligations with respect to Client Personal Data (as defined in Section 6) are set forth in Section 6 rather than in this Section 5. Nothing in this Agreement will limit use of information: (a) previously known to a Party without an obligation of confidentiality; (b) independently developed by or for a Party without use of the other Party's Confidential Information; (c) acquired by a Party from a third party which was not, to such Party's knowledge, under an obligation of confidentiality; or (d) publicly available through no breach of this Agreement. If a Party receives a subpoena or other valid legal process requiring disclosure of the other Party's Confidential Information, such Party may comply to the extent required by law and will, unless restricted by law, promptly notify the other Party and reasonably cooperate (at the other Party's request and expense) in opposing such a demand. The obligations included in this Section 5 shall

be applicable during the term of this Agreement and will survive after its termination.

6. Data Protection and Personal Data.

6.1 Definitions. Defined terms used in this Section 6, shall have the meanings given in Schedule 1.

6.2 "Client Personal Data" means Personal Data which is owned or controlled by Client, and which is provided by Client to Avanade for Processing according to Client's instructions for the purpose and during the provision of the Services, including, without limitation, data that is explicitly defined as a regulated category of data under Data Privacy Laws applicable to the Client. Except as expressly specified in the applicable SOW, the Parties acknowledge and agree that Avanade will not access Client Personal Data as part of the Services (excluding Business Contact Data such as name, telephone number, address, and email alias, as defined in the Data Processing and Security Addendum) and both Parties will use commercially reasonable efforts to monitor and restrict such access. However, if Avanade determines it has received Client Personal Data from Client that is not required to perform the Services, Avanade will notify Client and return or destroy such Client Personal Data (as instructed by Client), and Client shall take steps to promptly rectify the situation to prevent recurrence. If it is agreed in the SOW that Avanade will process Client Personal Data in connection with the Services, the general responsibilities of the Parties (with respect to the nature and purpose of such access, security controls and protocols, international transfer of data, etc.) as set out in the Data Processing and Security Addendum at Schedule 1 of this Agreement and the applicable SOW shall apply to the processing of such Client Personal Data.

7. Warranties.

7.1 Warranties.

Avanade warrants that it will perform the Services in a good and workmanlike manner. Avanade will re-perform Services that do not materially meet the foregoing warranty if Client notifies Avanade in writing within 30 calendar days of performance. Avanade warrants that the Deliverables will materially conform to the requirements set forth in the SOW for 30 calendar days from delivery to Client and will use commercially reasonable efforts to correct any non-conforming Deliverable if Client notifies Avanade in writing of the noncompliance within such period. The above warranties do not apply to any noncompliance resulting from (a) Client IP; (b) Third Party Products; (c) Avanade's reliance on a Client responsibility; (d) Client's use of Deliverables in production prior to acceptance or other than in accordance with applicable documentation or design; (e) modification, damage or other action of Client or any third party; or (f) combination with hardware, software, technology, services or other items not supplied or approved by Avanade. Avanade does not warrant that the Deliverables are free from non-material bugs, errors, defects or deficiencies that do not impact the performance of the Deliverables. The remedies set forth in this Section 7.1 are Client's sole and exclusive remedies and Avanade's sole and exclusive liability for breach of the warranties set forth in this Section 7.1. All other warranties, representations, conditions, indemnities, guarantees or other terms with respect to the Services, whether express or implied (including any implied warranty or condition of reasonable care and skill) are expressly excluded.

7.2 Disclaimer.

Except as set forth in Section 7.1, the Services, Deliverables, Avanade IP and other items provided by Avanade are provided "as is". Avanade does not make any other representations, warranties or covenants of any kind, whether express or implied, arising by law or otherwise, with respect to the Services, Deliverables, Avanade IP or other items provided by Avanade (including any implied warranty of merchantability, fitness for a particular purpose, quality, accuracy, title, or noninfringement and any implied warranty arising from course of performance, course of dealing, or usage of trade). Except as the Parties agree in writing, Avanade's warranties, obligations and liabilities and Client's

remedies for Third Party Products are limited to any recourse available against such third party.

8. Indemnity.

8.1 Infringement.

Each Party will defend and indemnify the other Party and its Affiliates, and their directors, officers and employees (each, an "**Indemnified Party**"), against any third party claims, costs or damages that may be awarded in a final judgment or agreed to by the indemnifying Party in a settlement of such claims:

(a) where Avanade is the indemnifying Party, a claim that any Deliverable provided by Avanade to Client pursuant to this Agreement: (i) infringes a copyright or trademark held by the third party; (ii) infringes the third party's patent existing as of the date of delivery of such Deliverable in any country in which the Services are delivered; or (iii) constitutes misappropriation or unlawful disclosure or use of the third party's trade secrets, except in each case to the extent such claims are based on: Client's modification or use other than as authorized by the SOW; Client's failure to use corrections or enhancements that Avanade made available; Client's combination with any product, technology or information not supplied or approved by Avanade; Client's distribution or use for the benefit of third parties; Avanade's compliance with Client specifications or requirements; or any Third Party Product, Client responsibility, or Client IP; and

(b) where Client is the indemnifying Party, a claim that any Client IP provided to Avanade pursuant to this Agreement: (i) infringes a copyright or trademark held by the third party; (ii) infringes a third party's patent existing as of the date of delivery to Avanade or Avanade's first use in any country in which the Client IP was provided or is used by Avanade; or (iii) constitutes misappropriation or unlawful disclosure or use of the third party's trade secrets.

8.2 Procedure; Remedies.

The Indemnified Party must promptly notify the indemnifying Party in writing of any indemnified claim and provide the Indemnifying Party reasonable cooperation and full authority to defend or settle the claim, provided that such settlement may not impose any obligation (monetary or otherwise) on the Indemnified Party without its consent. If any Deliverable is, or in Avanade's opinion is likely to be, held to infringe, Avanade will, at its expense, either (a) procure the right for Client to continue using it; (b) replace it with a non-infringing equivalent; (c) modify it to be non-infringing; or (d) direct its return, and refund to Client the Fees paid for it. The remedies in this Section 8 are the sole and exclusive remedies and each Party's entire liability with respect to infringement.

9. Limitations of Liability.

9.1 No Consequential Damages.

Neither Party will be liable for any incidental, consequential, special, indirect, punitive or exemplary damages (including loss of profit, reputation, data, share value, business or use), regardless of the form of action (whether in contract or tort or otherwise), whether the possibility of such damages has been disclosed or is reasonably foreseeable.

9.2 General Limitation of Liability.

Each Party's aggregate liability for claims arising from or in connection with this agreement, regardless of the theory of liability (whether in contract, tort or otherwise), will not exceed the fees paid by client under the SOW in the 12 months preceding the claim. This limitation does not apply to a breach of the confidentiality obligations in Section 5, the indemnity obligations under Section 8, client's payment obligations under this Agreement, or any other liability which cannot be excluded by law. This Section 9.2 specifically excludes claims involving

Client Personal Data, which are subject to the limitation in Section 9.3.

9.3 Client Personal Data Limitation of Liability.

Avanade's aggregate liability for claims involving Client Personal Data arising from or in connection with this agreement, regardless of the theory of liability (whether in contract, tort or otherwise), will not exceed the fees paid by client under the SOW in the 12 months preceding the claim.

10. Term and Termination.

The term of this Agreement commences on the Effective Date and continues until terminated as set forth below. Either Party may, subject to any terms in the SOW, terminate the SOW for convenience upon 30 calendar days written notice. Either Party may also terminate the SOW if the other Party does not cure the SOW related material breach within 30 calendar days of written notice by the Party identifying the breach. Termination of the SOW for material breach does not terminate any other SOW unless such material breach also constitutes a material breach under those other SOW(s). In the event of any termination of the SOW, Client will pay Avanade for all Services and Deliverables rendered under such SOW including a pro-rated portion for Deliverables in progress, and expenses incurred prior to the date of termination. Upon termination of the SOW by Client for convenience or by Avanade for breach, Client will also pay any reasonable demobilization costs. All provisions of this Agreement or the SOW which are by their nature intended to survive expiration or termination will survive such expiration or termination.

11. Dispute Resolution.

In the event of a dispute arising out of or relating to this Agreement, the Parties will consult and negotiate in good faith to reach a satisfactory solution within 30 calendar days. If the Parties do not resolve the dispute within such period, each Party may pursue such other remedies to which it is entitled.

12. Miscellaneous.

12.1 Notices.

Any notice or other communication provided under this Agreement will be in writing, addressed to such Party at the address set out in this Agreement, or upon electronic delivery by confirmed means.

12.2 Independent Contractors.

Each Party is an independent contractor and not a partner or agent of the other Party. Neither Party is authorized to enter into or incur any agreement, contract, commitment, obligation or liability in the name of or on behalf of the other Party.

12.3 Use of Name.

Client permits Avanade to use its name, logo and a brief description of the services being provided in external communications such as client listings, marketing materials and presentations. The listing will exclude Client-specific project information unless otherwise agreed by Client.

12.4 Alliance Relationship Disclosure; Communication with Affiliates.

Avanade is owned by Accenture and Microsoft. As a result of this relationship, Avanade is primarily dedicated to providing solutions to clients using Microsoft products and platforms. Avanade works closely with Microsoft on marketing and technical matters to promote solutions using the Microsoft platform and receives compensation and other benefits resulting from its Microsoft alliance and activities associated with its promotion of Microsoft products. Avanade's Microsoft certifications are dependent on Microsoft's verification of Avanade's work as a Microsoft partner. Accordingly, Client consents to Avanade sharing Client's name, contact information for a Client representative, and general information about the Services with Microsoft and Accenture. If contacted by Microsoft, Client agrees to provide reasonably requested information relating to Avanade's performance of the Services.

12.5 Non-Solicitation.

During performance of the Services and for 1 year thereafter, neither Party will, directly or indirectly, solicit the employment of the employees or contractors of the other Party who were introduced to such Party as a result of this Agreement, provided that this provision shall not apply to individuals who respond to general ads placed by a Party which were not specifically targeted to such individuals.

12.6 Non-Performance.

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 any of its responsibilities described in the Agreement, Avanade (i) shall be excused from failure to perform any affected obligations under the Agreement, (ii) shall be entitled to a reasonable extension of time considering the particular circumstances, and a reasonable reimbursement of additional costs incurred as a result, and (iii) shall not be responsible for any consequence or liability arising from Client's failure. Each Party will notify the other as promptly as practicable after becoming aware of the occurrence of any such condition.

12.7 Assignment.

Neither Party may assign this Agreement or the SOW, other than to an Affiliate or a successor by way of merger, acquisition, consolidation or corporate reorganization upon written notice to the other Party, without the written consent of the other Party, which will not be unreasonably withheld or delayed. This Agreement will be fully binding upon, inure to the benefit of, and be enforceable by the Parties and their successors and assigns.

12.8 Applicable Law.

This Agreement will be interpreted, construed and enforced in accordance with the laws of England and Wales, without reference to its rules relating to choice of law. Each Party irrevocably submits to the jurisdiction of the courts of England.

12.9 Compliance with Laws.

Each Party shall comply with applicable local laws and regulations that pertain to each Party's operation of its business and specific industry. Each Party will comply with all export control and sanction laws (collectively, "Trade Control Laws") applicable to its performance under this Agreement, including the use and transfer of any products, software, technology or services subject to this Agreement (collectively, "Items"). Without limiting the foregoing, neither Party shall transfer any Items: (i) to any geography subject to comprehensive economic sanctions (including without limitation the embargoed regions in Ukraine, Belarus, Cuba, Iran, North Korea, Russia or Syria) (each a "Restricted Geography")); (ii) to any party in violation of applicable Trade Control Laws; or (iii) that require government authorization to use or transfer without first obtaining: (a) the informed consent of the other Party; and (b) the required authorization. Avanade may decline in its sole discretion to engage in any activity under this Agreement with any connection to a Restricted Geography, or that Avanade otherwise determines could constitute a violation of applicable Trade Control Laws, without creating any liability on its part under this Agreement.

12.10 Electronic Signatures; Counterparts.

The Parties expressly agree that the SOW may be electronically signed, and that such signatures will be governed by the laws, policies and regulations of individual countries, regions, and industries. The SOW may be executed in counterparts, each of which when executed will be deemed an original, and such counterparts together will constitute one instrument.

12.11 Entire Agreement; Interpretation.

In the event of a conflict between any provision of this Agreement and any provision of the SOW, the provision of the SOW will control. This Agreement and the SOW, constitutes the entire agreement, and supersedes any and all prior agreements between the Parties with respect to the subject matter of this Agreement. This Agreement and the SOW cannot be amended or modified except in a writing that

specifically refers to this Agreement or the SOW signed by the authorized representatives of each Party. The authorized representative who may execute an amendment on behalf of Avanade is the Avanade signatory below, or a substitute representative at the same level or higher within Avanade. Conflicting or supplemental terms contained in any purchase order, online agreement (including click-wrap, browse-wrap, click-through, etc.), or any other document not meeting the requirements of this Section 12.11 are of no force or effect. The delay or failure of either Party to enforce the other Party's performance of any provision of this Agreement or exercise any right or remedy under this Agreement will not be interpreted or construed as a waiver of that Party's right to assert or rely upon such provision, right or remedy. This Agreement does not prohibit or restrict (a) either Party's right to perform services for any third party, including services comparable or similar to the Services or (b) the placement of resources involved in the performance or use of the Services. This Agreement exists for the benefit of the Parties only, and only the Parties may enforce it. The Parties do not intend for this Agreement to confer any right or benefit on any third party.

TERMS AND CONDITIONS

SCHEDULE 1

Data Processing and Security Addendum

This Data Processing and Security Addendum ("**Addendum**") describes the responsibilities of the parties with respect to the processing and security of any Client Personal Data in connection with the Services provided under the SOW. This Addendum is subject to the terms and conditions of the Agreement between Avanade and the Client. Terms not defined below shall have the meaning set forth in the Agreement.

1. **Definitions**.
   (a) "Business Contact Information" means the names, mailing addresses, email addresses, and phone numbers regarding the other Party's employees, directors, vendors, agents and clients, maintained by a Party for its own business purposes as further described in Section 9 below.
   (b) "Client Personal Data" means Client-owned or controlled personal data provided by or on behalf of Client to Avanade or an Avanade affiliate or subcontractor for processing under the SOW. Unless prohibited by applicable Data Protection Laws, Client Personal Data shall not include information or data that is anonymized, aggregated, de-identified and/or compiled on a generic basis and which does not name or identify a specific person.
   (c) "Data Protection Laws" means all applicable data protection and privacy Laws that apply to the processing of personal data under a particular SOW, including, as applicable, the EU General Data Protection Regulation 2016/679 ("GDPR"), the Federal Data Protection Act of 19 June 1992 (Switzerland), the UK Data Protection Act 2018 (as amended), and any US state or federal Laws or regulations pertaining to the collection, use, disclosure, security or protection of personal data, or to security breach notification, e.g., the California Consumer Privacy Act of 2018 ("CCPA").
   (d) "Information Security Incident" means a breach of Avanade's security leading to the accidental or unlawful destruction, loss, alteration or unauthorized acquisition, disclosure, misuse or access to unencrypted Client Personal Data transmitted, stored or otherwise processed by Avanade.
   (e) "Sub-processors" means third parties authorized under the terms of this Addendum to have access to and process Client Personal Data in order to provide a portion of the Services.
   (f) The terms "controller," "data subject," "de-identification," "personal data," "process," "processing," "processor," "pseudonymize," "sale," "service provider" and "supervisory authority" as used in this Addendum have the meanings given to any equivalent terms in the applicable Data Protection Laws, as relevant.

2. **Roles of the Parties; Compliance with Data Protection Laws**.
   (a) Each Party will comply with the requirements of the Data Protection Laws as applicable to such Party with respect to the processing of the Client Personal Data.
   (b) Client warrants to Avanade that it has all necessary rights to provide the Client Personal Data to Avanade for the processing to be performed in relation to the Services and agrees that Client shall be responsible for obtaining all necessary consents, and providing all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the Client Personal Data.
   (c) Avanade will process the Client Personal Data only in accordance with Client's documented processing instructions as set forth in the Agreement, including this Addendum and the SOW, unless otherwise required by law.
   (d) If Avanade is acting as a sub-processor in relation to any Client Personal Data (i.e., the data owner/controller is an entity other than Client), Client warrants to Avanade that Client's instructions with respect to the Client Personal Data have been authorized by the applicable data owner/controller, including the appointment of Avanade as a sub-processor.
   (e) Except as otherwise set forth in the SOW, (i) Avanade is a service provider and/or processor with respect to the Client Personal Data; and (ii) Client is an owner / controller or service provider / processor, as applicable, of the Client Personal Data.
   (f) The SOW shall set out (i) the subject matter and duration of the processing; (ii) the nature and

purpose of the processing; and (iii) the type of personal data and categories of data subjects involved.

(g) Avanade will promptly notify Client if Avanade determines, in its reasonable business judgment, that a Client processing instruction violates any applicable Data Protection Law (provided that nothing herein shall require Avanade to provide legal or regulatory advice or monitor Data Protection Laws as they apply to Client). In such event, the Parties will work together in good faith to resolve such issue in a timely manner. In no event will either Party be required to perform any activity that violates any applicable Data Protection Law. If Client requires that Avanade follow a processing instruction despite Avanade's notice that such instruction may violate an applicable Data Protection Law, Client will be responsible for all liability for all claims and damages arising from any continued processing in accordance with such instruction.

3. **Disclosure and Use of Data**.

(a) When providing or making available Client Personal Data to Avanade, Client shall only disclose or transmit Client Personal Data that is necessary for Avanade to perform the applicable Services.

(b) Following expiration or termination of the provision of Services relating to the processing of Client Personal Data, or at Client's request, Avanade shall (and shall require that its sub-processors) promptly and securely delete (or return to Client) all Client Personal Data (including existing copies), unless otherwise required or permitted by applicable laws. Unless otherwise agreed, Avanade will comply with any Client deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.

(c) In the course of providing the Services, Avanade may anonymize, aggregate, and/or otherwise de-identify Client data ("**De-Identified Data**") and subsequently use and/or disclose such De-Identified Data for the purpose of research, benchmarking, improving Avanade's offerings generally, or for another business purpose authorized by applicable Data Protection Law provided that Avanade has implemented technical safeguards and business processes designed to prevent the re-identification or inadvertent release of the De-Identified Data.

(d) All Avanade personnel, including subcontractors, authorized to process the Client Personal Data shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.

4. **Security Obligations**.

(a) Each Party shall implement appropriate technical and organizational security measures to safeguard Client Personal Data from unauthorized processing or accidental loss or damage, as further described in **Attachment 1** to this Addendum ("**Data Protection Protocols**").

(b) Taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Data, as well as the likelihood and severity of risk to individuals, Avanade's implementation of and compliance with the security measures set forth in **Attachment 1** is designed to provide a level of security appropriate to the risk in respect of the processing of the Client Personal Data.

5. **Additional Avanade Responsibilities**.

(a) **Documentation, Audits and Inspections**. Avanade shall make available to Client information reasonably requested by Client to demonstrate Avanade's compliance with its obligations in this Section and submit to audits and inspections by Client (or Client directed third parties) in accordance with a mutually agreed process designed to avoid disruption of the Services and protect the confidential information of Avanade and its other Clients. As required by applicable law, Avanade shall inform Client if, in Avanade's opinion, any Client audit instruction infringes upon any applicable Data Protection Law. Client shall be solely responsible for determining whether the Services and Avanade's security measures as set forth in **Attachment 1** will meet Client's needs, including with respect to any Data Protection Laws.

(b) **Data Subject and Supervisory Authority Requests**. As required by law and taking into account the nature of the Services provided, Avanade shall:

(i) provide assistance to Client as reasonably requested with respect to Client's obligations to respond to requests from Client's data subjects as required under applicable Data Protection Laws. Avanade will not independently respond to such requests from Client's data subjects, but will refer them to Client, except where required by applicable Data Protection Law; and

(ii) provide assistance to Client as reasonably requested if Client needs to provide information (including details of the Services provided by Avanade) to a competent supervisory authority, to the extent that such information is solely in the possession of Avanade or its Sub-processors.

(c) **Privacy / Data Protection Impact Assessments**. As required by law and taking into account the nature of the Services provided and the information available to Avanade, Avanade shall provide assistance to Client as reasonably requested with respect to Client's obligations to conduct privacy / data protection impact assessments with respect to the processing of Client Personal Data as required under applicable Data Protection Laws.

6. **Sub-processors**.

Client specifically authorizes the engagement of Avanade's affiliates as Sub-processors and generally authorizes the engagement of other third parties as Sub-processors as identified in the SOW. Avanade shall contractually require (including via intra-company agreements with respect to affiliates) any such Sub-processors to comply with data protection obligations that are at least as restrictive as those Avanade is required to comply with hereunder. Avanade shall remain fully liable for the performance of the Sub-processor. Avanade shall provide Client with written notice of any intended changes to the authorized Sub-processors and Client shall promptly, and in any event within 10 business days, notify Avanade in writing of any reasonable objection to such changes. If Client's objection is based on anything other than the proposed sub-processor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the parties shall be resolved via the contract dispute resolution procedure.

7. **Cross-Border Transfers of Client Personal Data**.

(a) **Transfers of EEA Data**. Subject to subsection (c) below, the parties shall rely on the EU Standard Contractual Clauses for the Transfers of Personal Data to Third Countries, dated 4 June 2021 (2021/914) as amended from time to time (the "EU Standard Contractual Clauses") to protect Client Personal Data being transferred from a country within the European Economic Area to a country outside the European Union not recognized by the European Commission as providing an adequate level of protection for personal data. Where the transfer relies on the EU Standard Contractual Clauses, the Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such EU Standard Contractual Clauses with the relevant Avanade entity or a third-party entity, acting as a data importer.

(b) **Transfers of non-EEA Data**. Subject to subsection (c) below, in the event that Client Personal Data is to be transferred from a country not within the European Economic Area to any other country in connection with the provision of Services under the Agreement, where required by applicable Data Protection Law, the parties shall enter into a data transfer agreement to ensure the Client Personal Data are adequately protected. Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such Data Transfer Agreement, with the relevant Avanade entity or a third-party entity, acting as a data importer.

(c) In the event that the transfer mechanisms agreed by the Parties herein are amended, replaced, or cease to be authorized as a means to provide "adequate protection" with respect to transfers of Personal Data, the Parties will work together expeditiously and in good faith to establish another valid transfer mechanism and/or implement supplementary measures as needed to establish appropriate safeguards for such data. Any impacts on the terms of the Agreement and the provision

of the Services caused by such new requirements will be addressed by the Parties in accordance with the Change Control Procedures.

(d) For avoidance of doubt and without prejudice to the rights of any data subjects thereunder, this Data Processing and Security Addendum and any EU Standard Contractual Clauses (or other data transfer agreements) that the Parties or their affiliates may enter into in connection with the Services provided pursuant to the Agreement will be considered part of the Agreement and the liability terms set forth in the Agreement will apply to all claims arising thereunder.

(e) **Intra-Group Agreements**. The processing and transfer of Personal Data (including cross border transfers) between Avanade and its Affiliates as sub-processors is facilitated and addressed by the Intra-Group Data Processing and Transfer Agreement executed between Avanade and its Affiliates.

8. **Information Security Incidents**. Avanade shall maintain procedures to detect and respond to Information Security Incidents. If an Information Security Incident occurs which may reasonably compromise the security or privacy of Client Personal Data, Avanade will promptly notify Client without undue delay. Avanade will cooperate with Client in investigating the Information Security Incident and, taking into account the nature of the Services provided and the information available to Avanade, provide assistance to Client as reasonably requested with respect to Client's breach notification obligations under any applicable Data Protection Laws.

9. **Use of Business Contact Information**. Each Party consents to the other Party using its Business Contact Information for contract management, payment processing, service offering, and business development purposes related to the Agreement and such other purposes as set out in the using Party's global data privacy policy (copies of which shall be made available upon request). For such purposes, and notwithstanding anything else set forth in the Agreement or this Addendum with respect to Client Personal Data in general, each Party shall be considered a controller with respect to the other Party's Business Contact Information and shall be entitled to transfer such information to any country where such Party's global organization operates.

10. **Changes in Laws**. In the event of (i) any newly enacted Data Protection Law, (ii) any change to an existing Data Protection Law (including generally-accepted interpretations thereof), (iii) any interpretation of a new or existing Data Protection Law by Client, or (iv) any material new or emerging cybersecurity threat, which individually or collectively requires a change in the manner by which Avanade is delivering the Services to Client, the Parties shall agree upon how Avanade's delivery of the Services will be impacted and shall make equitable adjustments to the terms of the Agreement and the Services in accordance with the Change Control Procedures.

TERMS AND CONDITIONS

Attachment 1 to Schedule 1

Data Protection Protocols

These Data Protection Protocols ("Protocols") set forth the security protocols that Client and Avanade will follow with respect to maintaining the security and privacy of Client Personal Data in connection with the Services that Avanade provides to Client under the SOW.

1. **General.** In the event of a conflict or inconsistency between the terms of the Agreement (including the SOW and documents referenced therein) and the terms of these Protocols, these Protocols will govern. Capitalized terms used herein, but not defined will have the meanings ascribed to them in the Agreement.

2. **Organizing Information Security.**

   2.1 Each Party will identify individuals who will be responsible for managing communications and confirming the implementation of and ongoing compliance with these Protocols on behalf of their respective organizations, namely the Accountable Managing Directors, Information Security Leads and Data Protection Officers. These individuals for each Party will be named in the SOW.

   2.2 Any communications related to these Protocols or the Parties' respective obligations regarding the security and privacy of Client Personal Data should be communicated in writing via e-mail or other written notice to each of the Accountable Managing Directors listed in the SOW. Further, the Accountable Managing Director or their designees will jointly review these Protocols no less frequently than once annually to determine whether any updates or revisions are recommended.

   2.3 Any changes to these Protocols are subject to the change control process set forth in the SOW.

   2.4 Each Party will be responsible for complying with each control designated as its responsibility in the table below, as the control relates to a Party's personnel and owned-equipment in its control and used to perform its respective obligations under the SOW.

TERMS AND CONDITIONS

Control		Responsible Party	
		Avanade	Client
1.	**Asset Management**		
1.1	**Acceptable Use of Assets**		
1.1.1	If Avanade devices will be used to access Client Personal Data, Avanade will require its Personnel to use these devices in accordance with Avanade's device usage procedures.	X	
1.1.2	Avanade will require its Personnel to comply with Client provided guidelines governing Avanade's use of any Client provided devices that may be used to access Client Personal Data as part of a project.	X	
1.1.3	Avanade will implement processes designed to require its subcontractors to comply with Avanade procedures governing the use of any subcontractor provided devices that may be used to access Client Personal Data.	X	
1.1.4	Avanade will require Client Personal Data to be securely removed from all Avanade or subcontractor devices assigned to the project prior to reassignment.	X	
1.1.5	Client will configure and maintain any Client provided devices, equipment, applications, infrastructure, or any other Client furnished items, provided to Avanade for use as part of any Services, in accordance with industry standards, including without limitation, updating such devices or equipment with the most up to date patches, signatures for anti-malware, firewalls, etc.		X
1.2	**Information Classification**		
1.2.1	Prior to performing any Services in connection with an applicable SOW, Client will notify Avanade if: (a) Avanade may have access, including incidental access, to Client Personal Data, or (b) Client Personal Data is being provided for Avanade to process as part of the Services. In either of the foregoing cases, Client will identify, classify and describe the classification restriction for any Client Personal Data clearly and appropriately.		X
2.0	**Human Resources Security**		
2.1	**Training**		
2.1.1	All Avanade Personnel will complete mandatory general security and privacy training no less frequently than once annually.	X	
2.1.2	Avanade Personnel will complete project specific training to address these Protocols as well as any Client specific requirements that may be set forth in the SOW.	X	
2.1.3	All Client personnel will complete training on these Protocols as well as any additional requirements that may be set forth in the SOW.		X
2.1.4	Avanade shall complete and maintain records within agreed timeframes designed to confirm that all Avanade Personnel comply with these Protocols upon rolling-on and rolling-off the project.	X	
3.0	**Physical and Environmental Security**		
3.1	**Physical Security**		
3.1.1	Client shall implement reasonable physical security controls at all Client locations where Client Personal Data is being processed in accordance with the Client's physical security standards.		X

TERMS AND CONDITIONS

Control		Responsible Party	
		Avanade	Client
3.1.2	Avanade shall implement reasonable physical security controls at Avanade facilities where Client Personal Data is processed in accordance with Avanade's security procedures (e.g., cable locks, screen locks, secure portable devices).	X	
3.1.3	Avanade shall conduct regular walk-throughs of Avanade corporate facilities used to process Client Personal Data to validate that applicable physical security controls are enforced.	X	
3.1.4	**In Avanade corporate offices utilized by Avanade to process Client Data, Avanade will implement the following or similar controls:**		
3.1.4.1	Each entry door to the facility will be closed and locked while Client Personal Data is in the facility.	X	
3.1.4.2	Avanade will implement a reasonable process to designate the Avanade Personnel that may access the facility. Only Avanade Personnel with a reasonable business need will be provided access to the facility.	X	
3.1.4.3	An electronic access control system utilizing authentication in line with industry standards will be installed on facility doors to enable such access control, unless access to the Avanade facility is controlled on a 24/7/365 basis by a guard.	X	
3.1.4.4	The access control system will be secured against tampering.	X	
3.1.4.5	The access control system will log the entry of Avanade Personnel for each time the door is accessed. Entry logs will contain a reliable time stamp, door location, and identification of the individual who gained access to the room.	X	
3.1.4.6	Avanade will periodically review access records to verify that access controls are being enforced effectively.	X	
3.1.4.7	If applicable, Avanade may review CCTV video storage to verify that access controls are being enforced effectively to prevent unauthorized entry.	X	
3.1.4.8	Avanade will assess its physical and environmental security controls at least annually and undertake internal review of the test results to determine whether control changes are needed.	X	
3.1.5	All Avanade Personnel shall be registered and required to carry appropriate ID badges when onsite at Avanade corporate facilities.	X	
4.0	**Communications and Operations Management**		
4.1	**Network Security Management (As applicable to each Party)**		
4.1.1	Access Control Lists (ACLs) shall be maintained for network devices.	X	X
4.1.2	Network traffic shall pass through firewalls that are monitored and protected by intrusion detection/prevention systems that allow traffic flowing through the firewalls to be logged.	X	X
4.1.3	Access to network devices for administration shall require a minimum of 256 bit encryption.	X	X
4.1.4	Avanade and Client will satisfy mutually agreed upon technical parameters (e.g., complexity guidelines, token lifetimes) for each other's network, application and server authentication credentials.	X	X
4.1.5	Where Client has provided devices to Avanade resources that permit access to Client Personal Data, Client will prevent such devices from having access to non-Client managed email solutions.		X

TERMS AND CONDITIONS

Control		Responsible Party	
		Avanade	Client
4.1.6	Anti-spoofing filters shall be enabled for email.	X	X
4.1.7	Transport Layer Security (TLS) between the Client and Avanade email domains shall be enabled.	X	X
4.2	**Virtual Private Networks ("VPN") and Remote Access. When remote connectivity to the Avanade network is required to process Client Personal Data and site to site VPN has been agreed upon, both Parties will deploy remote access services with the following or similar capabilities:**		
4.2.1	Avanade and Client will each encrypt connections between the two Parties using a minimum industry accepted standard and appropriate encryption technology.	X	X
4.2.2	Avanade and Client will each require the use of multi-factor authentication when access to the Client's network from non-Client or non-Avanade locations is permitted as part of the project.	X	X
4.3	**Data Storage and Handling of Client Personal Data**		
4.3.1	When storage of Client Personal Data on digital mobile media is required, Avanade and Client will require the data stored on the mobile media to be encrypted using an industry standard encryption technology.	X	X
4.3.2	If Avanade will access any Client Personal Data as part of the Services, prior to providing such access when possible in the context of the Services to be delivered by Avanade, Client shall pseudonymize, mask, de-identify or anonymize all such Client Personal Data prior to delivering or providing access to Avanade, and Client must identify in the SOW which of the foregoing data transformation measures Client has implemented.		X
4.3.3	If unmasked/unscrambled Client Personal Data will be accessible by Avanade, Client must identify in the SOW all such unmasked/unscrambled Client Personal Data together with any applicable compensating controls that the Parties agree will be used to mitigate Avanade's access to such unmasked/unscrambled Client Personal Data.	X	X
4.4	**Physical Transport of Data**		
4.4.1	Avanade and Client shall each use professional or government sponsored couriers for any third-party transport of hard copy or mobile media (using an industry standard encryption technology) containing Client Personal Data when transmitting such data.	X	X
4.5	**Data Disposal**		
4.5.1	Avanade will securely delete, destroy, and/or return, if feasible, any Client Personal Data no longer required in connection with the project.	X	
4.5.2	Avanade may retain archival copies of records containing Client Personal Data as reasonably necessary or as part of normal backup processes to verify Avanade's compliance with the Agreement, or as required by applicable law or regulation. Avanade shall not be obligated to retain archival copies of Client databases, or other compilations of Client Personal Data.	X	
4.5.3	Client shall advise Avanade of any data erasure or retention requirements based upon any applicable law or regulation.		X
4.5.4	Avanade shall destroy hard copies containing Client Personal Data via crosscut shredder or by deposit in a secure shred bin.	X	
5	**Access Control**		
5.1	**User Access Management**		

TERMS AND CONDITIONS

Control		Responsible Party	
		Avanade	Client
5.1.1	Management of Client and Avanade user accounts within Avanade systems shall follow Avanade's corporate access control procedures.	X	X
5.1.2	During the course of a project, Client shall periodically verify that no Client Personal Data will be processed under the SOW other than the categories and types described in the SOW.		X
5.1.3	Avanade will, during the course of the project, implement user account creation and deletion processes and controls, with appropriate approvals, for granting and revoking access to all Avanade systems and applications that store or enable access to Client Personal Data. In addition, Avanade shall designate an appropriate authority (as defined by the engagement) to approve creation of new user IDs, or elevated level of access for existing user IDs.	X	
5.1.4	Client will, during the course of the project, implement user account creation and deletion processes and controls, with appropriate approvals, for granting and revoking access to all Client systems and applications that store or enable access to Client Personal Data. In addition, Client shall designate an appropriate individual (as defined by the engagement) to approve creation of new user IDs, or elevated level of access for existing IDs.		X
5.1.5	Avanade shall maintain a roster documenting access rights related to all Avanade Personnel as appropriate; including level, type of access authorized, date access was granted and date access was revoked or terminated.	X	
5.1.6	Avanade will review the ACL at least quarterly, or as otherwise agreed to by the Parties in writing, to confirm that access levels are still appropriate for individual roles and to confirm that access revocations for Avanade Personnel who departed from the engagement have been processed correctly.	X	
5.1.7	Avanade and Client will grant system access to Avanade Personnel using the concept of Least Privileged Access, meaning individuals are only granted access to those resources and systems that are required to perform their role.	X	X
5.1.8	Avanade and Client will logically separate access between environments (e.g., development, testing, and production) using the concept of Least Privileged Access.	X	X
5.1.9	Avanade will revoke access of Avanade Personnel departing the project within 2 business days of departure, or as otherwise specified in the SOW, unless circumstances require immediate revocation.	X	
5.1.10	Before commencement of the project, Client will designate one or more specific individuals to administer, manage, and document Client systems or application access requests on behalf of Avanade Personnel who request access to Client Personal Data.		X
5.1.11	Avanade will appoint an individual who is separate from all other requestors and who is accountable for approving user IDs.	X	
5.1.12	Avanade and Client will require that individuals accessing systems and applications within their respective control use unique user login credentials.	X	X
5.1.13	Avanade will verify the source of any request for a login credential change before reissuing.	X	
5.1.14	Avanade will provide notification to the individual when he/she is assigned to a system administrator role.	X	
6	**Credential Management**		

TERMS AND CONDITIONS

Control		Responsible Party	
		Avanade	Client
6.1	Avanade and Client will each securely store authentication credentials.	X	X
6.2	Avanade and Client will communicate user credentials in a secure manner, ensuring account/user IDs are separate from the authentication. Avanade and Client will require that electronic communications of user credentials to be encrypted using an industry standard encryption technology. Avanade and Client will securely store the Avanade user login credentials (in password vault, key vault, or equivalent).	X	X
6.3	Avanade and Client will require that their respective project personnel change initial login authentication credentials upon their first logon attempt. Avanade and Client will also prohibit their respective personnel from sharing user login credentials.	X	X
6.4	Avanade will require that Avanade system administrators change their user login credentials every 30 days. In addition, Avanade will require that administrator passwords must be significantly different from the previous 12 passwords.	X	
6.5	Avanade will require that its Personnel use distinctive user login credentials for different systems (e.g., Client, Avanade, personal).	X	
7	**System Administrator**		
7.1	Avanade will maintain a log of all system administrators. System administrators will then maintain application-level ACLs that may contain additional details beyond what is in the project ACL (e.g., user IDs, levels of heightened access).	X	
7.2	Avanade will provide notification in writing to any individual assigned to a system administrator role so that the individual is aware of the privileged level of access that he or she has been granted.	X	
8	**Encryption**		
8.1	Avanade and Client will transmit Client Personal Data to one another using industry accepted encryption technology, when such data is not secured through another method.	X	X
8.2	Avanade will require that all workstations controlled by Avanade that are used to perform the Services (e.g., Avanade, rental, subcontractor workstations) are protected by full hard disk encryption using industry standard encryption technologies.	X	
8.3	Client will require that all workstations provided to Avanade by Client to perform the Services are protected by full hard disk encryption using industry accepted encryption technologies.		X
9	**Information Security Incident Management**		
9.1	**Security Incident Reporting**		
9.1.1	Avanade will require that its Personnel report to a centralized management response center (Avanade Asset Protection AAP@avanade.com) any Security Incident that may involve the loss or unauthorized acquisition of any Client Personal Data (e.g., a lost or stolen laptop).	X	
9.1.2	Client and Avanade will notify one another of any Security Incident which has resulted in the loss or unauthorized acquisition of any Client Personal Data (e.g., a lost or stolen laptop).	X	X
9.1.3	Client and Avanade will identify any additional Security Incident notification requirements that may be required, and are set forth in the SOW.	X	X

TERMS AND CONDITIONS