

## 1. INTERPRETATION

### 1.1 The definitions and rules of interpretation in this Clause apply in this Agreement.

**Applicable Data Protection Laws:** means i) to the extent the UK Data Protection Legislation applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data and ii) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Supplier is subject, which relates to the protection of personal data.

**Applicable Laws:** means i) to the extent the UK Data Protection Legislation applies, the law of the United Kingdom or of a part of the United Kingdom and ii) to the extent EU GDPR applies, the law of the European Union or any member state of the European Union to which the Supplier is subject.

**Background Materials:** means all Intellectual Property Rights, know-how, information, methodologies, techniques, tools, schemata, diagrams, ways of doing business, trade secrets, instructions manuals and procedures (including, but not limited, to software, documentation, and data of whatever nature and in whatever media) owned, developed or controlled by the Supplier which may have been created outside the scope, or independently of, this Agreement, and including all updates, modifications, derivatives or future developments thereof.

**Business Day:** a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

**Client:** means the name of the client as set out on the Grey Matter Cloud Service Contract.

**Client Data:** any information that is provided by the Client to the Supplier as part of the Client's use of the Managed Services, including any information derived from such information.

**Client-side Equipment:** any equipment located or to be located on a Client Site but controlled or to be controlled exclusively by the Supplier as part of the Managed Services.

**Client Site:** any premises used by the Client at which it receives the Managed Services.

**Client's Operating Environment:** the Client's computing environment (consisting of hardware and software) that is to be used by the Client in connection with its use of the Managed Services and which interfaces with the Supplier's System in order for the Client to receive the Managed Services, but excluding the Client-side Equipment.

**Commissioner:** the Information Commissioner (see section 114, DPA 2018).

**Confidential Information:** all confidential information (however recorded or preserved) disclosed by a Party or its employees, officers, representatives, advisers or subcontractors involved in the provision or receipt of the Managed Services (together, its **Representatives**) to the other Party and that Party's Representatives in connection with this Agreement which information is either labelled as such or should reasonably be considered as confidential because of its nature and the manner of its disclosure.

**CSP Agreement:** terms which govern the use of any Microsoft Licences (**Subscriptions**) purchased by the Client from the Supplier and which are directly flowed down from the Supplier's agreement with Microsoft® as set out in <https://www.microsoft.com/licensing/docs/customeragreementand> for financial sector the terms of the addendum set out at Schedule 2 and as updated from time to time by Microsoft®.

**Data Controller:** shall mean the Client;

**Data Processor:** shall mean the Supplier (which may include other affiliates within the Supplier's group) which has agreed to receive Personal Data from the Data Controller for further processing in accordance with the terms of this Agreement.

**Data Processor Personnel:** means the Data Processor and each of its Sub-Processors, and the officers, employees, agents, consultants, representatives and other personnel of each of the Data Processor and each Sub-Processor.

**Deliverables:** means all Documents, products and materials developed by the Supplier or its agents, subcontractors, consultants and employees in relation to the Managed Services in any form, including computer programs, data, reports and specifications (including drafts).

**Document:** means, in addition to any document in writing, any drawing, map, plan, diagram, design, picture or other image, tape, disk or other device or record embodying information in any form.

**EU GDPR:** the General Data Protection Regulation ((EU) 2016/679).

**Fees:** the fees payable to the Supplier, as described in the Grey Matter Cloud Service Contract.

**Good Industry Practice:** the standards that fall within the upper quartile of a skilled and experienced provider of business-critical managed services similar or identical to the Managed Services, having regard to factors such as the nature and size of the Parties, the term, the pricing structure and any other relevant factors.

**Hardware:** all physical telecommunications, networking and computer equipment (including switches, routers, cables, servers, racks, cabinets and peripheral accessories) provided and used by the Supplier to deliver the Managed Services to the Client.

**Initial Term:** 12 months from the date set out in the Grey Matter Cloud Service Contract.

**Intellectual Property Rights:** any and all intellectual property rights of any nature, whether registered, registerable or otherwise, including patents, utility models, trademarks, registered designs and domain names, applications for any of the foregoing, trade or business names, goodwill, copyright and rights in the nature of copyright, design rights, rights in databases, moral rights, know-how and any other intellectual property rights that subsist in computer software, computer programs, websites, documents, information, techniques, business methods, drawings, logos, instruction manuals, lists and procedures and particulars of Clients, marketing methods and procedures and advertising literature, including the "look and feel" of any websites, and in each case all rights and forms of protection of a similar nature or having equivalent or similar effect to any of these that may subsist anywhere in the world, in each case for their full term, together with any future rights and renewals or extensions.

**IPR Claim:** means a claim arising from the infringement of Intellectual Property Rights belonging to third parties.

**Main Agreement:** means the terms of this Agreement but excluding the CSP Agreement.

**Managed Services:** the services, as described in the Grey Matter Cloud Service Contract including any support arrangements and Online Services as applicable, to be performed by the Supplier in accordance with this Agreement.

**Normal Business Hours:** 8.00 am to 5.30 pm local UK time on Business Days.

**Online Services:** means any of the Microsoft-hosted online services subscribed to the Client under this Agreement, including Microsoft Dynamics Online Services, Office 365 Services, Microsoft Azure Services, or Microsoft Intune Online Services and which terms are governed by the CSP Agreement.

**Parties:** means the Supplier and the Client and each shall be a **Party**.

**Purpose:** the purposes for which the Relevant Personal Data is processed, as set out in Schedule 1.

**Grey Matter Cloud Service Contract:** means the order form which describes the type of Subscriptions, the support offering and the payment details. The Grey Matter Cloud Service Contract shall form part of the terms of this Agreement and shall be sent under separate cover.

**Request:** shall mean a request (including without limitation a subject access request or an erasure and porting request) from a Data Subject to exercise its rights under the Data Protection Legislation in respect of the Relevant Personal Data.

**Relevant Personal Data:** means all Personal Data processed by the Data Processor on behalf of the Data Controller under or in connection with the Agreement.

**Software:** any software used by the Supplier to provide the Managed Services to the Client whether owned by the Client (**Client Software**) or by the Supplier (**Supplier Software**) or Third Party Software (as defined below).

**Sub-Processor:** means a person or entity subcontracted by the Data Processor to process Relevant Personal Data in accordance with the Data Processor's obligations under or in connection with the Agreement which shall include Wayside Technology Group, Inc. For the avoidance of doubt, this shall exclude Third Party Processors.

**Supplier:** **GREY MATTER LIMITED** incorporated and registered in England and Wales with company number 1671407 whose registered office is at The Old Maltings, 2 Prigg Meadow, Ashburton, Devon, TQ13 7DF.

**Supplier's System:** the system to be used by the Supplier in performing the Managed Services, including the Hardware, the Software, the Client-side Equipment and communications links between the Hardware and the Client-side Equipment and the Client's Operating Environment.

**Third Party Processors:** means third parties who are not Sub-Processors and who have either a direct contract with the Client either through an end user licence agreement or other contractual arrangements and/or who are not in the direct control and supervision of the Supplier including Microsoft.

**Third Party Software:** any code or software programs written or provided by Microsoft<sup>®</sup> or other third parties which are used by the Client.

**UK Data Protection Legislation:** all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

**UK GDPR:** the EU GDPR as it applies in the UK after the end of the transition period (as set out in Article 126 of the EU-UK Withdrawal Agreement) by virtue of section 3 of the European Union (Withdrawal) Act 2018.

- 1.2 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.
- 1.3 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

- 1.4 A reference to **writing** or **written** includes e-mail.
- 1.5 In the event of any conflict or inconsistency between the Grey Matter Cloud Service Contract and the Clauses to this Agreement (including any changes to the schedules or additions or variations to the schedules), the following order of precedence shall apply (in decreasing order) to the extent of such conflict or inconsistency:
- (a) the Grey Matter Cloud Service Contract (as set out under separate cover);
  - (b) the Clauses.
- 1.6 For the avoidance of doubt, the terms set out in the CSP Agreement govern the rights and responsibilities of the Client and the Supplier in relation to the use of the Subscriptions and Online Services. All other Supplier services which falls outside the Subscriptions and Online Services are governed by the terms of the Main Agreement and shall take precedence over the terms of the CSP Agreement should any conflict arise over the use of the Supplier services.
- 2. SERVICE PROVISION**
- 2.1 The Supplier will provide the Managed Services with all due care, skill and ability as from the Initial Term unless earlier terminated for any reason.
- 2.2 The Supplier shall provide the Managed Services in accordance with the Grey Matter Cloud Service Contract.
- 2.3 Supplier does not and cannot control the flow of data to or from its network and other portions of the internet. Such flow depends in large part on the performance of internet services provided or controlled by third parties. At times, actions or omissions of such third parties can impair or disrupt connections to the internet (or portions thereof). Whilst the Supplier will use reasonable efforts to take all actions it deems appropriate to remedy and avoid such events, the Supplier cannot guarantee that such events will not occur. Accordingly, the Supplier disclaims any and all liability resulting from or related to such events.
- 2.4 The Client confirms that the Supplier may employ sub-contractors without seeking the prior consent of the Client (and any such sub-contractors shall be treated as the Supplier's employees for the purposes of this Agreement). Notwithstanding the foregoing, the Supplier shall at all times be responsible for and liable in respect of the performance of all obligations under this Agreement, whether such obligations are performed by the Supplier itself, or any sub-contractor engaged by the Supplier.
- 2.5 The Client shall not knowingly store, distribute or transmit any material through the Managed Services that:
- (a) is unlawful, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive;
  - (b) facilitates illegal activity;
  - (c) depicts sexually explicit images; and/or
  - (d) promotes unlawful violence, discrimination based on race, gender, age, disability, sexual orientation, religion and belief, gender reassignment, or any other illegal activities.

- 2.6 The Client shall remain responsible for the use of the Managed Services under its control, including any use by third parties that Client has authorised to use the Managed Services.
- 2.7 The Client must take reasonable measures to ensure it does not jeopardise services supplied to third parties on the same shared access infrastructure as notified to the Client by the Supplier in writing. This includes informing the Supplier promptly in the case of a denial-of-service attack or distributed denial-of-service attack. In the event of any such incident, the Supplier will work with the Client to alleviate the situation as quickly as possible. The Parties shall discuss and agree appropriate action (including suspending the Managed Services).
- 2.8 The Client shall not provide the Managed Services to third parties unless otherwise indicated in the Grey Matter Cloud Service Contract.
- 2.9 The Supplier reserves the right to:
- (a) modify the Supplier's System, its network, system configurations or routing configuration; or
  - (b) modify or replace any Hardware or Software in its network or in equipment used to deliver any Managed Service over its network,

provided that this has no adverse effect on the Supplier's obligations or performance under this Agreement and its provision of the Managed Services. If such changes will have an adverse effect, the Supplier shall notify the Client and the Parties shall follow the a change control process.

### **3. CLIENT DATA**

- 3.1 The Supplier shall promptly notify the Client in writing of any loss or damage to the Client Data. In the event of any loss or damage to Client Data, the Supplier shall use commercial reasonable endeavours to restore the lost or damaged Client Data from the latest backup of such Client Data. Subject to Clause 2.4, the Supplier shall not be responsible for any loss, destruction, alteration or unauthorised disclosure of Client Data caused by any third party.
- 3.2 The Parties shall comply with all obligations under Schedule 1 (**Data Protection Principles**).

### **4. SUPPLIER'S OBLIGATIONS**

- 4.1 The Supplier warrants that the Managed Services will be performed with all reasonable skill and care and that it will be provided in accordance with the terms and conditions of this Agreement.
- 4.2 The warranty in Clause 4.1 shall not apply to the extent of any non-conformance that is caused by use of the Managed Services contrary to the Supplier's instructions.
- 4.3 If the Managed Services do not conform with the warranty in Clause 4.1, the Supplier shall, at its expense, use commercially reasonable endeavours to correct any such non-conformance promptly, or provide the Client with an alternative means of accomplishing the desired performance.

- 4.4 Notwithstanding the foregoing, the Supplier does not warrant that the Client's use of the Managed Services will be uninterrupted or error-free.
- 4.5 This Agreement shall not prevent the Supplier from entering into similar Agreements with third parties, or from commissioning, engaging, independently developing, using, selling or licensing materials, products or services that are similar to those provided under this Agreement.
- 4.6 The Supplier shall:
- (a) staff the Supplier support desk with a team of skilled individuals;
  - (b) be a bona fide licensed user of all Third Party Software and of the Supplier's Software;
  - (c) use commercially reasonable endeavours to follow the instructions of the Client and will remain courteous during any communications with Client personnel;
  - (d) provide the Client with all necessary co-operation in relation to this Agreement;
  - (e) comply with all applicable laws and regulations with respect to its activities under this Agreement, including those set out in Clause 16; and
  - (f) carry out all other Supplier responsibilities set out in this Agreement or in any of the schedules in a timely and efficient manner.
- 4.7 The Supplier shall be under no obligation to provide the Managed Services to the Client in the following circumstances;
- (a) unauthorised use of the Software by the Client or use otherwise than in accordance with this Agreement;
  - (b) providing the Managed Services outside Normal Business Hours unless otherwise agreed between the Parties in writing;
  - (c) providing any other services not covered herein; and
  - (d) training in use of any upgrades; and
  - (e) providing the Managed Services to the Client where such support have been unnecessary if the Client had implemented update(s) and upgrade(s) supplied or offered to the Client pursuant to the call for technical support.

## **5. SECURITY**

- 5.1 The Supplier shall ensure that appropriate safety and security systems and procedures are maintained and enforced to prevent unauthorised access or damage to any and all Managed Services, the Supplier's System and related networks or resources and the Client Data, in accordance with Good Industry Practice.
- 5.2 Each Party shall promptly inform the other if it suspects or uncovers any breach of security, and shall use all commercially reasonable endeavours to promptly remedy such breach.

## 6. CLIENT'S OBLIGATIONS

- 6.1 To the extent that the Supplier requires access to the Client's Operating Environment to perform the Managed Services, the Client shall use reasonable endeavours to provide such access during Normal Business Hours and to provide a suitable work environment to enable the Supplier to perform such Managed Services subject to the Supplier complying with such internal policies and procedures of the Client (including those relating to security and health and safety) as may be notified to the Supplier in writing from time to time.
- 6.2 The Client shall:
- (a) use the Managed Services only for lawful purposes and in accordance with this Agreement;
  - (b) fully virus-check all data supplied to the Supplier pursuant to this Agreement;
  - (c) make Client's Operating Environment and Client-side Equipment, required to provide the Services, accessible to the Supplier's support staff, enable logons or passwords required for such support staff; and provide appropriate hardware interface, software and access authorisation to enable remote diagnosis, should such capability be required;
  - (d) provide all information and make available all resources as reasonably requested by Supplier in the execution of its obligations under this Agreement;
  - (e) use best efforts to follow the instructions of Supplier support personnel and will remain courteous during any communications with Supplier personnel;
  - (f) gather all relevant information prior to requesting assistance including detailed fault description, and procedures required to replicate a problem if possible. Any additional information which may help in the diagnosis of a fault should be included such as network configuration details;
  - (g) agree that if, in the course of performing the Managed Services, it is necessary or desirable for the Supplier to access or use any Client owned equipment, Client Software or Client Data (or which is in the possession of the Client) then it shall where it is able to under the terms of its existing licences grant to Supplier a non-exclusive, royalty free licence, during the term of the Agreement to use the same solely for the purpose of delivering the Managed Services;
  - (h) comply with all applicable laws and regulations with respect to its activities under this Agreement, including those set out in Clause 16; and
  - (i) carry out all other Client responsibilities set out in this Agreement or in any of the schedules in a timely and efficient manner. In the event of any delays in the Client's provision of such assistance as agreed by the Parties, the Supplier may adjust any timetable or delivery schedule set out in this Agreement as reasonably necessary.
- 6.3 The Client agrees and acknowledges to adhere to the terms of the CSP Agreement which govern the use of the Subscriptions and the Online Services.
- 6.4 In the event that the Client is in breach of its obligations under the Agreement (including payment obligations) then the Supplier shall provide written notice of such breach, specifying in detail the nature of the breach and providing thirty (30) Business Days' notice to remedy such breach if capable of remedy. If the Client fails to remedy such breach the Supplier shall be entitled to terminate or suspend the Managed Services without prejudice to any pre-existing rights and obligations of either Party. The Supplier shall have

no liability or responsibility should the Managed Services fail to comply as a direct result of the Client (including without limitation any of its employees, subcontractors or any of its staff) being in breach of the Agreement.

## **7. WARRANTIES**

7.1 The Client warrants that:

- (a) it has the full capacity and authority to enter into and perform this Agreement and that this Agreement is executed by a duly authorised representative of the Client;
- (b) it will comply with and use the Managed Services in accordance with the terms of this Agreement and all applicable laws, and shall not do any act that shall infringe the rights of any third party including the publishing or transmission of any materials contrary to relevant laws or in breach of the CSP Agreement;
- (c) it owns or has obtained valid licences, consents, permissions and rights to use, and where necessary to licence to the Supplier, any materials reasonably necessary for the fulfilment of all its obligations under this Agreement, including any third party licences and consents in respect of any Client Software; and
- (d) the Supplier's use in the provision of the Managed Services or otherwise in connection with this Agreement of any third-Party materials, including any Hardware or Software supplied by the Client to the Supplier for use in the provision of the Managed Services or otherwise in connection with this Agreement, shall not cause the Supplier to infringe the rights, including any Intellectual Property Rights, of any third party.

7.2 The Supplier warrants and represents that:

- (a) it has the full capacity and authority to enter into and perform this Agreement and that this Agreement is executed by a duly authorised representative of the Supplier;
- (b) it will comply with all applicable laws in performing its obligations under this Agreement;

## **8. CHARGES AND PAYMENT**

8.1 The Client shall pay the Fees for the Managed Services in accordance with an official Supplier quote as set out in the Grey Matter Cloud Service Contract. In the event of a conflict between the official Supplier quote and the Grey Matter Cloud Service Contract, the quote on the Grey Matter Cloud Service Contract shall prevail.

8.2 All amounts and Fees stated or referred to in this Agreement are exclusive of value added tax, which shall be added to the Supplier's invoice(s) at the appropriate rate.

8.3 Each invoice is due and the undisputed portion payable by direct debit as per the terms of the Grey Matter Cloud Service Contract. The Supplier be entitled to charge interest on all undisputed amounts, such interest to accrue on any overdue amounts at the rate of four (4) % over the base lending rate of the Royal Bank of Scotland, commencing on the due date and continuing until fully paid, whether before or after the judgment.



8.4 For Reserved Instance Subscriptions, the Client agrees and acknowledges that:

- (a) Reserved Instance Subscriptions will automatically renew
- (b) A 12% early termination fee may apply for cancelled reservations
- (c) The refund you receive for a cancellation is the remaining pro-rated balance minus the 12% early termination fee
- (d) The total refund amount cannot exceed \$50,000 USD in a 12-month rolling window
- (e) Refunds are calculated based on the lowest price of either your purchase price or the current price of the reservation
- (f) Only reservation owners can process a refund

## 9. CHANGE CONTROL

If either Party wishes to change the scope of the Managed Services it shall submit details of the requested change to the other in writing.

## 10. PROPRIETARY RIGHTS

- 10.1 Subject to Clause 10.2 below, on creation by the Supplier and upon the Supplier receiving payment in full, all Intellectual Property Rights in bespoke materials or code created under the Managed Services ("**Bespoke IPR**") for the Client shall vest automatically on creation in the Client. Supplier hereby assigns to the Client its present and future rights and full title and interest in such creations, including but not limited to workflows, widgets, business processes, and customised web coding which are used in order to provide the Managed Services. The Client hereby provides a irrevocable, worldwide, royalty-free licence to the Supplier for the duration of this Agreement to use such Bespoke IPR strictly for the purposes of providing the Managed Services.
- 10.2 Notwithstanding Clause 10.1 above, the Supplier shall retain exclusive ownership of (i) all of its Background Materials; and (ii) ideas, concepts, techniques and know-how discovered, created or developed by the Supplier during the performance of the Managed Services that are of general application and that are not based on or derived from the Client's business or Confidential Information ("**General IP**", together with the Background Materials, the "**Supplier Intellectual Property**"). The Supplier grants to the Client a non-exclusive, irrevocable, worldwide royalty free and non-transferable license to use the Supplier Intellectual Property.
- 10.3 The Client shall pay and indemnify Supplier on demand, from and against all actions, claims, liabilities, demands, proceedings, costs suffered or incurred by Supplier, arising by reason of claims that (1) Supplier's possession of or use of the Client's Intellectual Property in connection with the provision of the Managed Services infringes the Intellectual Property Rights of a third party; (2) the Client or any of its clients, modify, alter, replace combine with any other data, code, documents or other software, which alters the Supplier's Intellectual Property and such alterations infringe the Intellectual Property Rights of a third party. This indemnity applies whether or not legal proceedings are instituted and, if such proceedings are instituted, irrespective of the means, manner or nature of any settlement, compromise or determination.

- 10.4 The Client shall promptly notify the Supplier if any IPR Claim or demand is made or action brought against the Client for infringement or alleged infringement of any third party right which may affect the provision of Deliverables.
- 10.5 Except to the extent that the Supplier should reasonably have known or advised the Client the foregoing provisions of Clause 10.4, the Supplier shall have no obligation or liability for any IPR Claim to the extent such IPR Claim arises from:
- (a) any use by or on behalf of the Client of the combination with any item not supplied or recommended by the Supplier where such use of the Deliverables directly gives rise to the claim, demand or action; or
  - (b) any modification carried out on behalf of the Client to any item supplied by the Supplier under this Agreement if such modification is not authorised by the Supplier in writing where such modification directly gives rise to a claim, demands or action.

## 11. CONFIDENTIALITY

- 11.1 Confidential Information does not include any information that:
- (a) is or becomes generally available to the public (other than as a result of its disclosure by the receiving Party or its Representatives in breach of this Clause);
  - (b) was available to the receiving Party on a non-confidential basis before disclosure by the disclosing Party;
  - (c) was, is or becomes available to the receiving Party on a non-confidential basis from a person who, to the receiving Party's knowledge, is not bound by a confidentiality Agreement with the disclosing Party or otherwise prohibited from disclosing the information to the receiving Party;
  - (d) was known to the receiving Party before the information was disclosed to it by the disclosing Party;
  - (e) the Parties agree in writing is not confidential or may be disclosed; or
  - (f) is developed by or for the receiving Party independently of the information disclosed by the disclosing Party.
- 11.2 Each Party shall keep the other Party's Confidential Information confidential and shall not:
- (a) use such Confidential Information except for the purpose of exercising or performing its rights and obligations under this Agreement (**Permitted Purpose**); or
  - (b) disclose such Confidential Information in whole or in part to any third party, except as expressly permitted by this Clause.
- 11.3 Each Party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of this Agreement.
- 11.4 The Client acknowledges that the Supplier's Confidential Information includes any designs, plans, software or other materials created by the Supplier in connection with the Managed Services and the Client agrees



not to make use of any such material for any purpose other than receipt of the Managed Services from the Supplier.

- 11.5 The Supplier acknowledges that the Client Data is the Confidential Information of the Client.
- 11.6 A Party may disclose the other Party's Confidential Information to those of its Representatives who need to know such Confidential Information for the Permitted Purpose, provided that:
  - (a) it informs such Representatives of the confidential nature of the Confidential Information before disclosure; and
  - (b) at all times, it is responsible for such Representatives' compliance with the confidentiality obligations set out in this Clause.
- 11.7 A Party may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority or by a court or other authority of competent jurisdiction provided that, to the extent it is legally permitted to do so, it gives the other Party as much notice of such disclosure as possible.
- 11.8 Each Party reserves all rights in its Confidential Information. No rights or obligations in respect of a Party's Confidential Information other than those expressly stated in this Agreement are granted to the other Party, or to be implied from this Agreement.
- 11.9 The provisions of this Clause 11 shall continue to apply for three (3) years after termination of this Agreement.

## **12. LIMITATION OF LIABILITY**

- 12.1 This Clause 12 sets out the entire financial liability of each Party (including any liability for the acts or omissions of its employees, agents and subcontractors) in respect of:
  - (a) any breach of this Agreement; and
  - (b) any representation, misrepresentation (whether innocent or negligent), statement or tortious act or omission (including negligence) arising under or in connection with this Agreement.
- 12.2 Except as expressly and specifically provided in this Agreement:
  - (a) the Client assumes sole responsibility for results obtained from the use of the Managed Services, and for conclusions drawn from such use. The Supplier shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to the Supplier by the Client in connection with the Managed Services, or any actions taken by the Supplier at the Client's direction; and
  - (b) all warranties, conditions and other terms implied by statute or common law are, to the fullest extent permitted by law, excluded from this Agreement.
- 12.3 Nothing in this Agreement excludes or limits either Party's liability for:

- (a) death or personal injury caused by negligence;
- (b) fraud or fraudulent misrepresentation; or
- (c) any other liability which cannot lawfully be excluded or limited.

12.4 Subject to Clause 12.3:

- (a) neither Party shall be liable to the other in contract, tort (including for negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution or otherwise for any loss of profits, loss of business, depletion of goodwill or similar losses, or pure economic loss, or for any indirect or consequential loss, costs, damages, charges or expenses however arising; and
- (b) the Parties' total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement shall be limited to one hundred percent (100%) of the price paid for the Managed Services during the twelve (12) months preceding the date on which the claim arose.
- (c) The Supplier's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with a breach of its obligations set out in Schedule 1 shall be limited to two hundred percent (200%) of the price paid or payable for the Managed Services. For the avoidance of doubt, a Party shall not be entitled to claim under Clause 11 (Confidentiality) for claims under Schedule 1 (Data Protection Principles).

### 13. TERM AND TERMINATION

13.1 This Agreement shall, unless terminated earlier in accordance with this Clause, automatically be extended for successive twelve (12)-month periods (**Extended Term**) at the end of the Initial Term and at the end of each Extended Term, unless a Party gives written notice to the other Party, not later than ninety (90) days before the end of the Initial Term or the relevant Extended Term, to terminate this Agreement at the end of the Initial Term or the relevant Extended Term, as the case may be.

13.2 Without prejudice to any rights that the Parties have accrued under this Agreement or any of their respective remedies, obligations or liabilities, either Party may terminate this Agreement with immediate effect by giving written notice to the other Party if:

- (a) the other Party commits a material breach of any material term of this Agreement (including, without limitation breach of any payment obligations) and (if such breach is remediable) fails to remedy that breach within a period of thirty (30) days after being notified to do so;
- (b) the other Party breaches any of the terms of Clause 3, Clause 6, Clause 11 or Clause 16;
- (c) the other Party suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986; or
- (d) the other Party suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business.

- 13.3 Termination of this Agreement, for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of the Parties existing at termination.
- 13.4 On termination of this Agreement for any reason:
- (a) the Supplier shall immediately cease provision of the Managed Services;
  - (b) the Client shall pay all outstanding sums owing to the Supplier up to and including the date of termination; and
  - (c) each Party shall use reasonable endeavours to return and make no further use of any equipment, property, materials and other items (and all copies of them) belonging to the other Party.
- 13.5 If a Party is required by any law, regulation, or government or regulatory body (**Regulatory Requirement**) to retain any documents or materials which it would otherwise be obliged to return or destroy, it shall notify the other Party in writing of such retention, giving details of the documents or materials that it must retain. Clause 11 shall continue to apply to any such retained documents and materials for as long as any such requirement continues in force, subject to any disclosure mandated by any Regulatory Requirement.

#### **14. STAFF TRANSFER AND NON-SOLICITATION**

- 14.1 It is not intended that any staff be transferred from the Supplier to the Client or from the Client to the Supplier pursuant to this Agreement or that any 'relevant transfer' occur for the purposes of the Transfer of Undertakings (Protection of Employment) Regulations 2006 ('the Regulations').
- 14.2 Neither Party shall solicit the other Party's staff or contractors who have been employed or engaged in the Managed Services or the performance of this Agreement during the lifetime of this Agreement and for a period of 9 months thereafter. For the purposes of this clause 'solicit' means the soliciting of such person with a view to engaging such person as an employee, director, sub-contractor or independent contractor.
- 14.3 In the event that either Party is in breach of clause 14.2 above then the Party in breach shall pay to the other by way of liquidated damages an amount equal to 50% per cent of the gross annual budgeted fee income (as at the time of the breach or when such person was last in the service of the relevant Party) of the person so employed or engaged. This provision shall be without prejudice to either Party's ability to seek injunctive relief.
- 14.4 The Parties hereby acknowledge and agree that the formula specified in clause 14.3 above is a reasonable estimate of the loss which would be incurred by the loss of the person so employed or engaged.

#### **15. FORCE MAJEURE**

- 15.1 The Supplier shall have no liability to the Client under this Agreement and the Client shall have no obligation to pay the Fees if the Supplier is prevented from, or delayed in, performing its obligations under this Agreement, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control except to the extent that the Supplier could reasonably have avoided such circumstances by fulfilling its obligations in accordance with the terms of this Agreement or otherwise exercising the level of diligence

that could reasonably have been expected of it (having exercised Good Industry Practice), including strikes, lock-outs or other industrial disputes (excluding any industrial disputes involving the workforce of the Supplier), act of God, pandemic, epidemic, war, riot, civil commotion, compliance with any law or regulation, fire, flood or storm (each a **Force Majeure Event**), provided that:

- (a) the Client is notified of such an event and its expected duration; and
- (b) the Supplier uses all reasonable endeavours to mitigate, overcome or minimise the effects of the Force Majeure Event concerned,

and that if the period of delay or non-performance continues for four (4) weeks or more, the Party not affected may terminate this Agreement by giving fourteen (14) days' written notice to the other Party.

## **16. ANTI-BRIBERY**

16.1 The Parties shall:

- (a) comply with all applicable laws, regulations and sanctions relating to anti-bribery and anti-corruption, including the Bribery Act 2010;
- (b) promptly report to the other Party any request or demand for any undue financial or other advantage of any kind received in connection with the performance of this Agreement.

## **17. WAIVER**

No failure or delay by a Party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it preclude or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

## **18. SEVERANCE**

18.1 If any court or competent authority finds that any provision of this Agreement (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this Agreement shall not be affected.

18.2 If any invalid, unenforceable or illegal provision of this Agreement would be valid, enforceable and legal if some part of it were deleted, the Parties shall negotiate in good faith to amend such provision such that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the Parties' original commercial intention.

## **19. ENTIRE AGREEMENT AND AMENDMENT**

19.1 This Agreement and the terms of the Grey Matter Cloud Service Contract constitutes the entire Agreement between the Parties and supersedes all previous discussions, correspondence, negotiations, arrangements, understandings and Agreements between them relating to its subject matter.

19.2 No alteration to or variation of this Agreement shall take effect unless and until the same is in writing and signed on behalf of each of the Parties by a duly authorised representative.

**20. ASSIGNMENT**

The Parties shall not, without the prior written consent of the other (which consent is not to be unreasonably withheld), assign, transfer, charge, subcontract or deal in any other manner with all or any of its rights or obligations under this Agreement.

**21. NO PARTNERSHIP OR AGENCY**

Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, nor authorise any Party to make or enter into any commitments for or on behalf of any other Party.

**22. THIRD-PARTY RIGHTS**

This Agreement is made for the benefit of the Parties to it and (where applicable) their successors and permitted assigns, and is not intended to benefit or be enforceable by anyone else.

**23. NOTICES**

23.1 Any notice or other communication required to be given to a Party under or in connection with this Agreement shall be in writing and shall be delivered by hand or sent by pre-paid first class post or other next working day delivery service, at its registered office (if a company) or (in any other case) its principal place of business.

23.2 Any notice or communication shall be deemed to have been received if delivered by hand, on signature of a delivery receipt, or otherwise at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service.

23.3 This Clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution. For the purposes of this Clause, "writing" shall not include e-mail.

**24. GOVERNING LAW AND JURISDICTION**

24.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be exclusively governed by and construed in accordance with the law of England.

24.2 The Parties irrevocably agree that the courts of England shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).



**25. COUNTERPARTS**

- 25.1 This Agreement may be executed in any number of separate documents or separate each in the like form, all of which taken together shall constitute one (1) and the same document, and either Party may execute this Agreement by signing any one (1) or more of such documents or counterparts (which may be facsimile copies).



## Schedule 1- Data Protection Principles

For the purpose of this Agreement, the words "**Data Subject**", "**Personal Data**", "**processing**", "**transfer**" (in the context of Personal Data transfers) and "**appropriate technical and organisational measures**" shall be interpreted in accordance with the applicable UK Data Protection Legislation.

- 1.1 Both Parties will comply with all applicable requirements of Applicable Data Protection Laws. This clause 1 is in addition to, and does not relieve, remove or replace, a Party's obligations or rights under Applicable Data Protection Laws
- 1.2 Without prejudice to the generality of paragraph 1.1, the Data Controller will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Relevant Personal Data to the Supplier as Data Processor for the duration and purposes of this Agreement.
- 1.3 In performance of its obligations under the Agreement, the Data Controller shall provide the Data Processor with complete and accurate details of the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of Personal Data and categories of Data Subject, as may be required to ensure compliance with the Data Protection Legislation and as more fully set out in Annex 1 (**Details of Personal Data Processed**). The Supplier shall not be deemed to have breached any of its obligations as Data Processor by virtue of a breach of the Data Protection Legislation by the Data Controller. The Supplier shall not be deemed liable for any claim including but not limited to a claim by a Data Subject arising from any action or omission by the Supplier to the extent that such action or omission resulted directly from the Data Controller's instructions.
- 1.4 The Parties shall, at all times, comply with the provisions and obligations imposed by the Data Protection Legislation and the data protection principles set out therein when processing Relevant Personal Data.
- 1.5 In processing Relevant Personal Data, the Data Processor shall (and will procure all the Data Processor Personnel shall):
  - (a) process that Relevant Personal Data only on the documented instructions of the Data Controller, unless the Data Processor is required by Applicable Laws to otherwise process that Relevant Personal Data. Where the Data Processor is relying on Applicable Laws as the basis for processing Relevant Personal Data, the Data Processor shall notify the Data Controller of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Data Processor from so notifying the Data Controller on important grounds of public interest. The Data Processor shall inform the Data Controller if, in the opinion of the Data Processor, the instructions of the Customer infringe Applicable Data Protection Laws;
  - (b) implement appropriate the technical and organisational measures to protect against unauthorised or unlawful processing of Relevant Personal Data and against accidental loss or destruction of, or damage to, Relevant Personal Data, which the Data Controller has reviewed and confirms are appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;

- (c) ensure that any personnel engaged and authorised by the Data Processor to process Relevant Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;
- (d) assist the Data Controller insofar as this is possible (taking into account the nature of the processing and the information available to the Data Processor), and at the Data Controller's cost and written request, in responding to any Request and in ensuring the Data Controller's compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- (e) notify the Data Controller without undue delay on becoming aware of a personal data breach involving the Relevant Personal Data;
- (f) at the written direction of the Data Controller, delete or return Relevant Personal Data and copies thereof to the Data Controller on termination of the Agreement unless the Data Processor is required by Applicable Law to continue to process that Relevant Personal Data. For the purposes of this paragraph 1.5(f) Relevant Personal Data shall be considered deleted where it is put beyond further use by the Data Processor; and
- (g) maintain records to demonstrate its compliance with this Schedule 1 and allow for reasonable audits by the Data Controller or the Data Controller's designated auditor, for this purpose, on reasonable written notice.

1.6 The Data Controller consents to the appointment of the Sub-Processor Wayside Technology Group, Inc.

1.7 The Data Controller hereby provides its prior, general authorisation for the Data Processor to:

- (a) appoint Sub-Processors to process the Relevant Personal Data, provided that the Data Processor:
  - (i) shall ensure that the terms on which it appoints such processors comply with Applicable Data Protection Laws, and are consistent with the obligations imposed on the Data Processor in this Schedule 1;
  - (ii) shall remain responsible for the acts and omission of any such processor as if they were the acts and omissions of the Data Processor; and
  - (iii) shall inform the Data Controller of any intended changes concerning the addition or replacement of the processors, thereby giving the Data Controller the opportunity to object to such changes provided that if the Data Controller objects to the changes and cannot demonstrate, to the Data Processor's reasonable satisfaction, that the objection is due to an actual or likely breach of Applicable Data Protection Laws, the Data Controller shall indemnify the Data Processor for any losses, damages, costs (including legal fees) and expenses suffered by the Data Processor in accommodating the objection.
- (b) transfer Relevant Personal Data outside of the UK as required for the Purpose, provided that the Data Processor shall ensure that all such transfers are effected in accordance with Applicable Data Protection Laws. For these purposes, the Data Controller shall promptly comply with any reasonable request of the Data Processor, including any request to enter into standard data protection clauses adopted by the EU Commission from time to time (where the EU GDPR applies



to the transfer) or adopted by the Commissioner from time to time (where the UK Data Protection Legislation applies to the transfer).

**Annex 1**  
**Details of Personal Data Processed**

<b>Data subjects:</b>	<p>Client personnel</p> <p>Client's clients</p> <p>Client third parties</p> <p>Business contacts in general</p>
<b>Types of personal data:</b>	<p>Name</p> <p>Job title</p> <p>Email address</p> <p>Phone number</p> <p>Business/home address</p> <p>Date of birth</p> <p>Place of birth</p> <p>Any other personal data provided by the Client to the Supplier</p>
<b>Special categories of personal data:</b>	None
<b>Purpose of processing:</b>	<p>In the case of data subjects other than staff: for the purpose of providing IT services and support to the Client's business.</p> <p>In the case of staff: for the purpose of providing IT services and support for the Client's employment and HR matters.</p>
<b>Nature of processing:</b>	As set out in the body of the Agreement.
<b>Additional instructions:</b>	None



## Schedule 2 FSI Addendum

# Microsoft Cloud Agreement Financial Services Amendment

This Financial Services Amendment (“Amendment”) is entered into between Customer and the Microsoft Affiliate who are parties to the Microsoft Cloud Agreement (the “Agreement”). The parties agree that this Amendment supplements the Agreement and applies only to the Online Services, defined below, that Customer buys under the Agreement.

Customer or Customer’s Affiliate is subject to oversight by a financial services Regulator. In consideration of such oversight, the parties agree that the Agreement is amended as follows:

### 1. Defined Terms

Capitalized terms used but not defined in this Amendment will have the same meanings as provided in the Agreement or the Online Services Terms (“OST”). The following definitions are used in this Amendment:

“Customer” means, for purposes of this Amendment, any Affiliates that are subject to oversight by a Regulator and are consuming Online Services.

“Microsoft Online Services FSI Customer Compliance Program” or “FSI Customer Compliance Program” means an optional, fee-based program available to Microsoft customers or affiliates of those customers that are subject to oversight by a Regulator.

“Online Services” means, for purposes of this Amendment, the Microsoft Dynamics 365 Core Services, Office 365 Services, Microsoft Azure Core Services, Microsoft Intune Online Services and Microsoft Power BI Services, each as defined in the “Data Processing Terms” section of the OST.

“Regulator” means any financial services regulator that has examination or supervisory rights over Customer or Microsoft as the provider of Online Services to Customer.

### 2. Enabling Customer Compliance

**a. Effective Access to Data and Business Premises.** As set forth in this Amendment and for clarity and to be consistent with applicable regulations, Microsoft will provide Customer, Customer’s internal and external auditors (both of which are defined as “Customer Auditor” herein) and Customer’s Regulator, with effective access to data related to the activities outsourced to Microsoft, as well as reasonable access to Microsoft’s business premises (see Section 2(b)(ii) and Section 2(c)(iii)). Customer will at all times have direct access to Customer Data, including Customer’s virtual machines and applications deployed in the Online Services. This includes the ability for Customer to conduct vulnerability and penetration testing of Customer’s deployments in the Online Services or other similar testing as applicable to a specific Online Service that Customer is using. For avoidance of doubt, Customer must conduct any testing in accordance with Microsoft’s terms and conditions, which may require, among other things, Customer to provide Microsoft with advance notice of any tests and prohibit Customer from targeting any other Microsoft customer.

#### **b. Regulator Right to Examine.**

(i) In the event that Customer’s Regulator requests information relating to Customer’s use of the Online Services, Customer will, in the first instance, use the standard features of the Online Services and the information provided to Customer to respond to such request.

(ii) In the event that the Regulator requests to examine the Online Services operations and controls in order to meet the Regulator’s supervisory obligations of Microsoft as a service provider of Customer, Microsoft will provide the Regulator with a direct right to examine the Online Services, including the ability to conduct an on-premises examination; to meet with Microsoft personnel and Microsoft’s external auditors; and to access any related information, records, reports and documents. Such activities may take place at Microsoft’s offices, at other locations where activities relating to the Online Services provided to Customer and its Affiliates are performed, and as otherwise requested by the Regulator.

(iii) Microsoft will not disclose Customer Data to the Regulator except as described in the General Privacy and Security Terms in the OST, and the Regulator will not be allowed access to data belonging to any other Microsoft customer.

(iv) Customer will at all times have access to Customer Data using the standard features of the Online Services and may delegate its access to Customer Data to representatives of the Regulator.

(v) Customer and Microsoft will be responsible for their own costs associated with any of the activities described in this Section 2(b).

(vi) For clarity, Microsoft and Customer will work together to resolve each Regulator request through discussion and interaction between Customer, Microsoft and the Regulator. Microsoft and Customer acknowledge that the provisions relating to the Regulator right to examine are not intended to contravene or interfere with any applicable



laws or regulations, and nothing in this section should be construed as an impediment to the Regulator's ability to examine the Online Services.

**c. Customer Examination, Monitoring and Audits Rights.** To enable Customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide Customer, and other customers that are subject to oversight by a Regulator, with access to information, Microsoft personnel and Microsoft's external auditors. Such rights and processes are designed to provide Customer with effectively the same access to information and personnel that Microsoft would provide to a Regulator, while preserving Microsoft's ability to operate the Online Services and protect the privacy and confidentiality of other customers' data. Specifically, Microsoft will provide Customer, including Customer Auditor, with the rights described below. The activities described in Section 2(c)(iii) below may occur onsite in Microsoft's offices or at other locations where activities relating to the Online Services are performed.

**(i) Online Services Information Security Policy.** As set forth in the OST, each Online Service follows a written data security policy ("Information Security Policy") that complies with certain control standards and frameworks. Microsoft will make each Information Security Policy available to Customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by Customer regarding Microsoft security practices and policies.

**(ii) Audits of Online Services.** On behalf of customers including Customer and Customer's Auditor, as well as any Regulator, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data) for each Online Service. Each audit will result in the generation of an audit report ("Audit Report"), as set forth in the OST. Pursuant to the terms set forth in the OST, if Customer requests, Microsoft will provide Customer with each Audit Report.

**(iii) FSI Customer Compliance Program.** Customer may participate in the optional FSI Customer Compliance Program at any time under this Agreement, which enables Customer to have additional monitoring, supervisory and audit rights and additional controls over the Online Services as described in Sections 2(c)(iii)(1) - (2) below.

**1) Supervisory Access to Online Services Information and Microsoft Personnel.**

**A. Additional Microsoft Support.** Through Customer's Premier Support Services engagement, Customer will have access to Microsoft personnel for raising questions and escalations relating to the Online Services.

**B. Audit Webcasts.** Subsequent to Microsoft receiving an Online Services Audit Report, Microsoft will invite all FSI Customer Compliance Program members ("Members") to participate in a webcast, hosted by Microsoft, for Members to discuss the results of the audit. Each webcast will include an assessment of whether: (1) the control procedures were suitably designed to provide reasonable assurance that the stated internal control objectives would be achieved if the procedures operated as designed, and (2) the control procedures operated effectively during the reporting period. Upon request from Members that attend the audit webcast, Microsoft will provide detailed information regarding planned remediation of any deficiencies identified by the audit.

**C. Significant Events.** Microsoft will provide communications to all Members regarding (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on Members' use of the Online Services; (2) Microsoft risk-threat evaluations; and

(3) significant changes to Microsoft's business resumption and contingency plans, or other circumstances, that might have a serious impact on Members' use of the Online Services.

**D. Penetration Testing.** At least annually, Microsoft will conduct third party penetration testing against the Online Services, including evidence of data isolation among

tenants in the multi-tenant Online Services. Upon request, Microsoft will provide Members with a summary report of the results of such penetration testing.

**E. Transparency of Online Services Through Program Events.** Microsoft will make subject matter experts for the Online Services available to all Members through group events such as webcasts or in-person meetings, including an annual summit event. Such events will include a roadmap of planned developments, an opportunity for Members to provide structured feedback and/or suggestions regarding the FSI Customer Compliance Program and its desired future evolution, and reports of significant events (as described in this section). These events will also provide an opportunity for Members to discuss common issues with each other and raise them with Microsoft. The format and frequency of community events may vary over time; provided, that the objectives set forth in this paragraph will be accomplished not less than annually.

**F. Additional Member Requests for Information.** For Online Services that have been audited pursuant to SSAE 16 SOC 1 Type II and SSAE 16 SOC 2 Type II, as reflected in the OST, Members may request additional information from Microsoft subject matter experts not addressed through the standard features of the Online Services, the provisions in Section 2 or other available resources, on a fee-based per diem basis. In order to respond to any such request, Microsoft will

prepare a statement of work with estimated fees, based on a per diem rate of US\$4,000 per day for each Microsoft employee, plus reasonable travel expenses. Members will not be charged the full per diem fee for a Microsoft engineering resource who is needed for only a portion of a single day. Microsoft will only charge fees for work performed on a pro rata basis. Further, Microsoft will not charge fees for any Microsoft employee performing administrative tasks, such as meeting coordination, escorting visitors or document copying. The statement of work must be executed by both parties before work can commence. Invoicing, payment and tax terms will be the same as for Professional Services under the Microsoft Premier Support Services Agreement.

If a Member is not reasonably satisfied by the sufficiency of the information provided by Microsoft employees, the Member may submit a written request to meet with one of Microsoft's external auditors. Microsoft will request that the external auditor that has audited the relevant Online Service meet with the Member to discuss any questions. Any such discussion will be subject to the agreement of the external auditor, will be at the Member's expense, and will be subject to the Member signing confidentiality documentation in form and content satisfactory to the external auditor.

## 2) Ability to Influence the Online Services and Programs – Suggestions for Additional Testing.

Microsoft will provide each Member with advanced details on existing and future certifications, audit plans and scope and will solicit feedback on any potential changes to current certifications. For each Microsoft audit, 100% of the existing controls in scope for that audit type will be subject to testing by the auditor, and the expectation is that all controls for each audit scope will be tested within a 3-year audit cycle. As part of the FSI Customer Compliance Program, each Member may suggest additional controls to be included in a future audit scope. Microsoft will consider each such suggestion and, if not accepted, will provide a reasoned basis for refusal. For any given audit cycle, across all suggestions from all Members, Microsoft will include a minimum of five Member-specified controls (from the existing control set) in the audit instructions and will inform the auditor that these controls were selected by the Members. Compliance with these controls will be validated using tests that are consistent with the type of audit (e.g., ISO or SSAE) undertaken.

If the total number of Members in the FSI Customer Compliance Program exceeds 15, Microsoft will establish an executive committee ("Executive Committee"). For a given audit cycle, the Executive Committee will determine the five controls described above on behalf of all Members. Microsoft may, at its discretion, include additional controls requested by Members.

The Executive Committee will be comprised of at least one representative from each key regulated market with a participant in the FSI Customer Compliance Program. If there are multiple Members from a given market, the Executive Committee member for that market will be determined by (1) majority agreement among the Members from that market that have more than 10,000 active seats in the Office 365 Services or more than US\$500,000.00

annual commitment of Microsoft Azure Core Services, or (2) a regulator having authority over all Members from that market. The key regulated markets shall, at a minimum, include Canada, United States, United Kingdom, France, Germany, Japan and Italy. Microsoft may add key regulated markets or increase the number of Members on the Executive Committee only in consultation with all Members.

For clarity, nothing in this section precludes Members from requesting that new controls or additional details for a given product, feature or Online Service be included in the roadmap for future audits. Microsoft will consider each such request and, if not accepted, will provide a reasoned basis for refusal.

## 3) FSI Customer Compliance Program Conditions and Processes.

**A. Conditions.** Customer's participation in the FSI Customer Compliance Program is conditioned on Customer (a) being regulated by a Regulator; (b) maintaining an active, paid subscription to one or more Online Services through the Agreement; and (c) maintaining an active, paid Microsoft Premier Support Services agreement. Customer also must pay a US\$50,000 annual fee for each year Customer participates.

**B. Onboarding.** If Customer decides to join the FSI Customer Compliance Program, an authorized Customer representative shall notify Microsoft by sending Customer contact information and purchase order details for the annual fee to the following Microsoft email address: [fsicomppro@service.microsoft.com](mailto:fsicomppro@service.microsoft.com).

**C. Termination.** Customer may terminate its membership in the FSI Customer Compliance Program at any time by notifying Microsoft. Microsoft may terminate Customer's membership in the FSI Customer Compliance Program if Customer fails to satisfy any of the conditions set forth in Section 2(c)(iii)(3)(A) above.

## 3. Security Incident: Limited Reimbursement for Certain Costs

To the extent that a Security Incident (as defined in the OST) results from Microsoft's failure to comply with its obligations under the Agreement, and subject to the limitations of liability applicable to each Online Service, Microsoft will reimburse Customer for reasonable out-of-pocket remediation costs incurred by Customer in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" consist of (a) actual costs of payments, fines, penalties, sanctions, attorneys' fees, court costs or fees, or other remedies or liabilities, and any interest thereon, imposed by a court, tribunal, arbitration panel, government body or regulatory agency for a Microsoft-caused Security Incident;

(b) additional commercially-reasonable out-of-pocket expenses incurred by Customer or its Affiliates to manage or remedy the Microsoft-caused Security Incident including, without limitation, costs associated with restoring, correcting, or repairing the affected Online Service; (c) commercially-reasonable out-of-pocket expenses for legally-required notifications of Customer's end users of



the Microsoft-caused Security Incident (but not the costs of any professional third-party services, including those relating to crisis management, public relations or media relations services, which are indirect and consequential damages under the Agreement). Customer must document all such expenditures and, upon Microsoft's request, those expenditures must be validated by an independent, internationally-recognized third party financial services industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Microsoft under this paragraph will be characterized as direct damages subject to the limitation on liability in the Agreement, and not as indirect, consequential, special or incidental damages excluded in the Agreement.

#### 4. Customer Termination Rights

- a. **Termination at the Direction of Regulator.** Customer may terminate an Online Service at the express direction of a Regulator with reasonable notice.
- b. **Termination for Regulatory Compliance.** In the event Customer becomes subject to a new government law, regulation, requirement, decision, order or other ruling that Customer determines it cannot comply with because Customer is using the Online Service(s), Microsoft will discuss with Customer how to accommodate Customer's requirements. The parties may contemplate adding additional products or services, procuring those products or services from a third-party provider, or adding other solutions, each at Customer's expense. If the parties are not able to satisfy Customer's new regulatory requirements, Customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice to Microsoft.

#### 5. Business Continuity of Online Services

Microsoft acknowledges that Customer may be required by its Regulator to ensure that it is able to continue to carry on its business in the event of (1) regulatory or other legal action impacting Customer or one of its Affiliates; or (2) termination of the Agreement. Microsoft and Customer agree as follows:

##### a. Continuity after Customer Transfer of Rights.

- 1) In the event of the insolvency, reorganization, liquidation or some other action impacting Customer or one of its Affiliates, as provided by applicable law or regulation for the financial industry (e.g., "too big to fail", "recovery and resolution", "special administration", and similar regulations and actions), and to the extent required to maintain continuity of Microsoft's provision of the Online Services purchased by Customer under the Agreement, Microsoft will consent to Customer assigning, sublicensing or transferring its rights under the Agreement to (A) one or more of its Affiliates, or (B) a third party that purchases or otherwise succeeds to any or all of the business or assets or equity of Customer. In each case, the entity to which rights are transferred is the "Transferee," and Transferee will have access to Customer Data through Microsoft's standard processes and tools.
- 2) Microsoft will neither terminate the Agreement nor suspend or delay the performance of its obligations under the Agreement, subject to the following conditions:
  - A. The Transferee must pay all fees and charges payable by Customer to Microsoft under the terms of the Agreement for services provided before the transfer and through the renewal or replacement of the Agreement.
  - B. The Transferee and Microsoft will work in good faith to renew the Agreement or, as appropriate, to replace the Agreement with appropriate terms for Microsoft to provide the Online Services to the Transferee.
  - C. If Microsoft and the Transferee cannot agree on terms, as described in clause B, within 12 months after the transfer of rights to Transferee, then Microsoft may terminate the Agreement by providing notice to Transferee.
  - D. The aggregate liability of Microsoft and its Affiliates to Customer, Customer's Affiliates and the Transferee will not exceed the aggregate liability of Microsoft and its Affiliates under the Agreement.
- 3) In the event the Transferee would like to enter into a new Agreement, the parties will work in good faith to put in place terms that are appropriate in light of the transfer under this Section 5(a).

**b. Continuity after Termination of Agreement.** If the Agreement terminates for any reason, then Customer may elect to extend the Online Services on a month-to-month basis for up to twelve months from the date of termination by providing notice of such election to Microsoft. During such period, Microsoft will continue to provide, and Customer will continue to receive and pay for, the Online Services pursuant to the terms and conditions of the Agreement. In addition, during such period Customer will be able to retrieve its Customer Data through Microsoft's standard processes and tools. Customer may cancel the extended service by providing a notice of cancellation to Microsoft. Cancellation will be effective at the end of the month following thirty days after Microsoft receives the notice of cancellation.

**c. Reversibility.** In the event of a termination of the Agreement as described in Section 4 and this Section 5 and Customer chooses to migrate to a different online service, Customer may request that Microsoft provide assistance in such transition through Microsoft's Professional Services Organization at the then-current rates for such services.

Customer may request migration or transition assistance and support from Microsoft's Professional Services Organization at any time during the extended service period described in Sections 5(a) and 5(b).





## 6. *Miscellaneous*

**a. Confidentiality.** This Amendment, the Information Security Policy, the Audit Reports, and all information regarding and provided through the FSI Customer Compliance Program are Microsoft Confidential Information. Customer may disclose these items to a Customer Auditor or consultant or a Regulator, provided that (1) Customer first redacts all terms that are unrelated to regulatory oversight and approval, including pricing information and order quantities; and (2) other than disclosures to a Regulator, Customer must comply with the Confidentiality terms of the Agreement as if the disclosure was a disclosure of Microsoft Confidential Information by Customer to a Customer Representative.

**b. Term and termination.** Subject to Section 4 and Section 5 above, this Amendment will terminate automatically upon any termination of the Agreement. Except for changes made by this Amendment, the Agreement identified above remains unchanged and in full force and effect. If there is any conflict between any provision in this Amendment and any provision in the Agreement identified above and any provision in the OST, this Amendment shall control.

### Schedule 3 - Surveil EULA

1. The End User Terms and Conditions located at <https://slim.azureedge.net/slim/eula.pdf> ("IT Exact Terms") apply to the provision of the IT Exact Software as a Service ("IT Exact Service") as between the Client and IT Exact Limited ("IT Exact"). In the event the Client does not accept the IT Exact Terms, the Supplier reserves the right to suspend the provision of the Services until such time as the Client accepts such IT Exact Terms.
2. IT Exact be solely responsible for its compliance with the IT Exact Terms.
3. The Supplier:
  - (a) expressly excludes any warranty to the Client that the IT Exact Service supplied or licensed under the Managed Services Agreement will operate substantially in accordance with, and perform, the material functions and features as set out in the its marketing, sales or other associated documentations; and
  - (b) shall not be liable to the Client:
    - (i) for the acts or omission of IT Exact; or
    - (ii) for any failure to perform its obligations under the Managed Services Agreement or this Order Form where there is a corresponding failure by IT Exact to perform its obligations under the IT Exact Terms.
4. The Client shall be liable to the Supplier for, and shall indemnify and keep the Supplier indemnified on demand against, any loss, damages, costs, expenses (including without limitation legal costs and expenses), claims or proceedings in respect of:
  - (a) any loss or damage that arise or result from the Client's breach of the IT Exact Terms; and
  - (b) the amount of all costs and expenses (including legal and out-of-pocket expenses) incurred by the Supplier in connection with enforcing or preserving any rights under, or monitoring the provisions of the IT Exact Terms.The Client's liability under this clause shall be unlimited.
5. The provision of the IT Exact Service referred to in this Order Form shall be solely governed by the IT Exact Terms. For the avoidance of any doubt, in the event of a conflict between the IT Exact Terms and the Managed Services Agreement or this Order Form insofar as it relates to the IT Exact Service only, the IT Exact Terms shall prevail. For all other Services, the Managed Services Agreement and this Order Form shall apply.