

## AWS Marketplace Addendum

This Addendum to the AWS Marketplace Standard Contract including its schedules ("**Addendum**") is made on the date of purchase of the Services on the AWS Marketplace (the "**Commencement Date**") between:

**SmartComms, SC Limited**, a company registered in England and Wales under number 4303041, having its registered office at Suite 23, LCLB, 95 Mortimer Street, London, WIW 7GB ("**SmartCom**"), and;

the entity purchasing the Services as detailed in the AWS Marketplace ("**Buyer**" or "**Customer**").

This Addendum contains the terms and conditions upon which the SaaS Services, Support and Consultancy Services are provided pursuant to the AWS Marketplace and incorporates the Standard Contract for AWS Marketplace terms set out in Schedule 5. Each Order shall specify the specific SaaS Services, Support and/or Consultancy Services to be provided to Buyer and/or Client and shall be deemed to be a separate agreement in respect of the SaaS Services, Support and/or Consultancy Services set out therein and incorporates the terms of the Agreement as if they were set out in full in each Order. In the event of any conflict between this Addendum and the Order, the Order shall prevail.

### Definitions.

"Administrators"	means those Users who have been designated by Customer as having administrative rights in respect of access to and use of a facility within the SmartCom Technology made available to Customer and User(s) as part of the SaaS Services;
"Allowance"	means amounts and levels of the SaaS Services specified in an Order permitted to be used by Customer during an Order Year;
"Annual Fees"	means the charge per twelve (12) month period specified in an Order (exclusive of any amounts payable as a result of Overage) for the right to access and use the SaaS Services up to the limits specified in such Order and receive the associated Support;
"Charges"	means Annual Fees, charges in respect of Overages, Consultancy Fees and any other charges payable by Customer to SmartCom;
"Community Page"	means SmartCom's on-line community page, as notified by SmartCom from time to time, currently located at: <a href="https://community.smartcommunications.com/s/article/DOC-6262">https://community.smartcommunications.com/s/article/DOC-6262</a> ;
"Consultancy Fees"	means the charges and expenses for provision of Consultancy Services set out in an applicable Statement of Work or SmartCom's daily rates as published from time to time;
"Consultancy Services"	means the provision during Office Hours of general consultancy services including: project management, delivery, installation, implementation, creation and/or implementation of a Statement of Work, and/or training; the initial amounts of which required by Customer and any timeframe for delivery all being as specified in an Order;
"Effective Date"	means the date of commencement of SaaS Services (and associated Support) or Consultancy Services as specified in an applicable Order;
"License Term"	means the initial period as specified in an Order for which Customer is authorized to access and use and commits to paying the Annual Fees which shall thereafter automatically renew for consecutive twelve (12) monthly periods unless either Party serves notice of non-renewal upon the other Party at least sixty (60) days before the end of the initial period specified in an Order or each anniversary thereof;
"Order"	means Buyer's subscription to the SaaS Services and commitment to pay the associated Charges by means of accepting a Public Offer or Private Offer via the submission process on the AWS Marketplace;
"Order Year"	means in respect of an applicable Order, each twelve (12) month consecutive period beginning from the commencement of the License Term;
"Overage"	means where the Volume exceeds the Allowance specified in an Order and/or the Usage Policy triggering additional fees at the rate also specified or otherwise referred to in an Order and/or other consequences as specified in the Usage Policy;
"Premium Support Fees"	means the fees due for the provision of Support provided on a 24x7 basis as specified in an Order;
"Private Offer"	means an offer specific to Buyer to purchase the Services specified therein submitted from SmartCom to Buyer via the AWS Marketplace;
"Public Offer"	means the offer to purchase the Services generally via the public page for the Services listed on the AWS Marketplace;
"SaaS Services"	means access to: (i) the relevant Solution provided via Customer's login link at the Website or another designated web site or IP address; (ii) ancillary online or offline products and services (other than Consultancy Services or Support) provided or licensed to Customer by SmartCom; and/or (iii) the content management system and any other product, service or license belonging to a Third Party; all as specified in an Order;
"SmartCom Technology"	means all proprietary technology belonging to or used by SmartCom and its affiliates (including software, hardware, products, processes, algorithms, user interfaces, know-how, techniques, designs and other tangible or intangible technical material or information) which is made available to Customer under an Order or is otherwise used by SmartCom to provide the SaaS Services;
"Solution"	means the particular SmartCom product(s) specified in an Order;
"Statement of Work" or "SOW"	means a written description of how the SaaS Services are to be deployed as may be jointly agreed and implemented as part of the Consultancy Services. A Statement of Work shall be construed as an Order as the context requires;
"Support"	means technical support for the SaaS Services of the type as specified in Schedule No. 1 (Support);
"Third-Party Application(s)"	means any products, services, material online applications and offline software products that interoperate with the SaaS Services that are provided or supported by third parties and are not provided by SmartCom;

<b>"User(s)"</b>	means the number of natural persons specified in an Order or otherwise permitted under such Order to use particular components of the SaaS Services;
<b>"User Guide"</b>	means the online user guide for the SaaS Services, accessible via login at the Website, as updated from time to time;
<b>"Volumes"</b>	means the actual amounts and levels of the SaaS Services used during an applicable Order Year by Customer and/or User(s);
<b>"Website"</b>	means <a href="http://www.smartcommunications.com">http://www.smartcommunications.com</a> and/or other domain names designated from time to time; and
<b>"Working Day" or "Office Hours"</b>	means 9 AM to 5 PM UK time Monday to Friday excluding UK public holidays.

1. **Orders.** Customer shall order the SaaS Services and Support by completing and signing an Order. Orders shall only be binding once signed by both parties and where applicable, a serial number issued which will allow Customer to download the software necessary to use the SaaS Services. At the end of the initial twelve months, and at the commencement of each Order Year thereafter, Buyer acknowledges that SmartCom may increase the Annual Fees by 5% above the fees pertaining to the previous Order Year. This Order is subject to the Usage Policy in Annex 1.

2. **User Guide.** Buyer shall use the SaaS Services in accordance with the User Guide.

3. **Community Page and Administrators.** SmartCom will provide Buyer with access to the Community Page for the purpose of receiving communications from regarding the SaaS Services (including notifications concerning SaaS Services downtime and updates). Buyer is responsible for ensuring that the appropriate Administrator(s) register and create user credentials in respect of registering for use of the Community Page and receiving notifications hereunder. Buyer shall: (i) provide SmartCom with up-to-date details of its Administrators (including a 'Primary Admin' person); Buyer agrees that only Administrators or its corporate officers have the authority to request SmartCom to make changes to a Tenancy and Buyer acknowledges that SmartCom may decline such requests if not made by an Administrator or corporate officer.

4. **Training.** Buyer is responsible for ensuring that its personnel are reasonably trained in using the SaaS Services and that the SaaS Services are used for their intended purpose and in accordance with the User Guide. In particular, Buyer agrees that it is responsible for its Users' compliance with the terms of this Addendum and an applicable Order.

5. **Privacy and Security Terms.** The parties agree that Schedule 2 (Data Protection and Privacy) and Schedule 3 (Security) shall apply.

6. **Third-Party Applications.** Buyer may choose to obtain Third-Party Applications for use with the SaaS Services. SmartCom assumes no responsibility for, and specifically disclaims any liability or obligation with respect to, any Third-Party Applications that are provided pursuant to the terms of the applicable third-party license or separate agreement between the licensor of the Third-Party Applications and Buyer. SmartCom does not represent and/or warrant in any manner that Third-Party Applications are accurate, current, or comply with laws, rules and/or regulations of, or are otherwise valid and enforceable in or appropriate for, the jurisdiction in which the Third-Party Applications are used or for Buyer's purposes. If Buyer uses Third-Party Applications with the SaaS Services, Buyer accepts that those Third-Party Applications will, in order to operate with the SaaS Services, access Buyer Data. SmartCom shall not be responsible for any disclosure, modification or deletion of Buyer Data resulting from any such access by Third-Party Applications. Service features that interoperate with Third-Party Applications depend on the continuing availability of the relevant API for use with the SaaS Services. If the providers of the Third-Party Applications cease to make the API available on reasonable terms for the Service, SmartCom may cease providing such Service features without entitling Buyer to any refund, credit, or other compensation. Buyer acknowledges that the availability and its use of the SaaS Services is conditional upon Buyer having a valid license to use the relevant Third-Party Application, where applicable.

7. **Back-up and Data Loss.** Buyer acknowledges that the SaaS Services are not intended or designed to be a system of record. Buyer is responsible for the input and maintenance of the Buyer Data and for maintaining effective back-up procedures as may be necessary to replace any Buyer Data in the event of loss. SmartCom shall not be responsible or liable for any loss or damage to, or failure to store, Buyer Data.

8. **Service Levels.** The parties agree that Schedule 4 (Service Levels) shall apply to the SaaS Services.

9. **Fees.** Except as expressly set forth in the applicable Order and/or Statement of Work, Buyer will pay all fees set forth in the applicable Order and/or Statement of Work in accordance with the following:

- a. the Annual Fees and, if applicable, Premium Support Fees, is payable annually in advance on the Effective Date and each anniversary thereafter during the License Term;
- b. Overages are payable as and when determined by SmartCom;
- c. the Consultancy Fees are payable as set out in a Statement of Work or in advance on the Effective Date if not set forth in a Statement of Work. SmartCom's fees are invoiced annually in advance, and the first invoice will coincide with the Order Start Date or effective date of a Statement of Work;
- d. payment will be due within thirty (30) days from the date of the invoice; and
- e. all amounts will be denominated in Great British Pounds (GBP)..

10. **No Refund.** Buyer acknowledges that the Charges are based on SaaS Services ordered and are due irrespective of whether or not Buyer utilizes the SaaS Services. Payment obligations are non-cancellable and Charges paid are non-refundable and the number of User subscriptions purchased cannot be decreased during the License Term.

11. **Offsets; Late Charges.** Buyer shall not be entitled to withhold or offset any amounts owed by SmartCom to Buyer that are not derived from this Agreement against any invoice issued under this Agreement.

12. **Overages.** SmartCom will calculate and record the Volumes for each calendar month during the License Term and in the event of an Overage SmartCom will provide Buyer with a written report specifying in reasonable detail the amount of Overage and the supplemental fees due in respect of such Overage. In this event, Buyer agrees to pay the supplemental fee calculated in accordance with the rates specified in an Order.

13. **Interest.** SmartCom reserves the right to: (i) charge Buyer interest in respect of the late payment of any sums due (before as well as after judgement) at the rate of 3% (or such other rate as may be specified in an Order) per annum above the base rate from time to time of Barclays Bank from the due date thereof until payment; and/ or (ii) suspend access to the SaaS Services and Support until full payment has been received by SmartCom.

14. **Disputed Invoices.** Should Buyer have any queries or bona fide dispute(s) regarding amount of any invoice issued by SmartCom it shall so notify SmartCom within twenty-one (21) days of the date of issue of the relevant invoice and provide reasonable grounds in respect of the

disputed amount. For the avoidance of doubt, all undisputed sums set out in an applicable invoice shall be paid in accordance with the invoice terms. Any bona fide dispute properly submitted with the above shall be escalated and dealt with by senior finance personnel from each Party and discussed in good faith for a period of up to ten (10) Working Days from the date of the escalation. If a dispute is resolved in favor of SmartCom, the disputed amount shall be paid within five (5) Working Days of the date of resolution. Should no resolution be reached by the Parties in accordance with the above, SmartCom shall be entitled to exercise its legal remedies to the fullest extent.

15. **Tax Responsibility.** All payments required by Agreement are stated exclusive of all taxes, duties, levies, imposts, fines or similar governmental assessments, including sales and use taxes, value-added taxes ("**VAT**"), goods and services taxes ("**GST**"), excise, business, service, withholding tax and similar transactional taxes imposed by any jurisdiction and the interest and penalties thereon (collectively, "**Sales Taxes**"). Buyer shall be responsible for and bear Sales Taxes associated with its purchase of, payment for, access to or use of the SaaS Services. Sales Taxes shall not be deducted from the payments to SmartCom, except as required by law, in which case Buyer shall increase the amount payable as necessary so that after making all required deductions and withholdings, SmartCom receives and retains (free from any tax liability) an amount equal to the amount it would have received had no such deductions or withholdings been made. If Buyer claims tax exempt status for amounts due under this Agreement, it shall provide SmartCom with a valid tax exemption certificate (authorized by the applicable governmental authority) to avoid application of Sales Taxes to Buyer's invoice. Each Party is responsible for and shall bear Sales Taxes imposed on its net income. Buyer hereby confirms that SmartCom can rely on the ship-to name and address set forth in the applicable Order and/or Statement of Work that Buyer places directly with SmartCom (or as subsequently notified by Buyer in writing), as being the place of supply for the assessment of Sales Taxes. Buyer shall notify SmartCom in writing of any changes to the ship-to name and address before the Commencement Date and shall be responsible and liable for any delay or error in such notification. The Parties' obligations under this Section (Tax Responsibility) shall survive the termination or expiration of this Agreement.

16. **Invoicing Taxes.** If SmartCom is required to invoice or collect taxes associated with Buyer's purchase of, payment for, access to or use of the SaaS Services, SmartCom will issue an invoice to Buyer including the amount of those taxes, itemized where required by law. If applicable, Buyer shall provide to SmartCom its VAT, GST or similar tax identification number(s) on the Order or SOW. Buyer shall use the ordered SaaS Services for Buyer's Business Use in the foregoing location(s) in accordance with the provided VAT or GST identification number(s).

17. **Expenses.** Buyer agrees that SmartCom's daily rates for provision of the Consultancy Services are exclusive of any expenses incurred by SmartCom while performing the Consultancy Services, including but not limited to reasonable travel and living expenses of SmartCom personnel, airfare, mileage, parking, tolls, lodging, auto rental and per diem meal expense; which Buyer agrees to pay upon production by SmartCom of suitable evidence such as receipts for the expenses being claimed.

18. **Usage Certification.** At SmartCom's request, Buyer shall promptly furnish SmartCom with written certification verifying that the SaaS Services are being used in accordance with the Order, including the number of Users. Buyer shall give SmartCom reasonable access to Buyer's records to verify that the SaaS Services are being used in accordance with the terms of the Order.

19. **Remedies cumulative.** Unless stated otherwise, any termination hereunder shall be without prejudice to any other rights or remedies either Party may be entitled to hereunder or at law or in equity and shall not affect any accrued rights or liabilities of either Party nor the coming into or continuance in force of any provision hereof which is expressly or by implication intended to come into or continue in force on or after such termination.

20. **Publicity.** Neither Party shall refer to the identity of the other Party in promotional material, publications, or press releases or other forms of publicity relating to the SaaS Services unless the prior written consent of the other Party has been obtained, provided, however, that SmartCom may use Buyer's name and logo for the limited purpose of identifying Buyer as a customer of the SaaS Services.

# Schedule No. 1 (Support)

## Contact Information

There are two ways to contact Support.

Email: support@smartcommunications.com  
Telephone: +1 800 986 6317

The preferred method of communication is email except that all Severity 1 and Severity 2 Errors must be reported to SmartCom by telephone. All communications with SmartCom customer support will be in English.

## Support Hours

Premium Support (24x7)

## Definitions

In addition to the terms defined in Section 1 of the Addendum the following terms shall have the following meanings:

“**Error**” means any material and reproducible failure of the SaaS Services to operate in accordance with the User Guide (but not the availability of the Service itself);

“**Error Severity Levels**” mean:

“**Severity 1**” or “**S1**” means a catastrophic failure of the SmartCom Technology which prevents SmartCom from providing the SaaS Services;

“**Severity 2**” or “**S2**” means a severe problem with the SmartCom Technology which causes serious disruption to Buyer’s use of the Solution in a production system;

“**Severity 3**” or “**S3**” means a moderate problem with the SmartCom Technology which causes the Solution not to operate as designed having only a moderate impact on Buyer’s use of the Solution;

“**Severity 4**” or “**S4**” means a minor problem or general query with the Solution; and

“**Severity 5**” or “**S5**” means a minor problem with the Solution which is logged and closed as a request for enhancement to be considered for incorporation in a future Upgrade;

“**Permanent Fix**” means the repair or replacement of object or executable code version of the Solution to remedy an Error;

“**Resolution**” or “**Resolution Time**” means the resolution of an Error by means of a Temporary Fix/Workaround or Permanent Fix within the times specified in the Error Severity Levels table below;

“**Response**” or “**Response Time**” means the elapsed clock time between: (i) SmartCom’s logging of an Error reported by Buyer; and (ii) SmartCom responding to Buyer in respect of that Error;

“**Service Levels**” means the Response Times to each Error Severity Level;

“**Upgrade**” means a modification or enhancement release, in object code form, containing new enhancements, features or functionalities. Upgrades are provided to Buyer by SmartCom at its discretion. Buyer is solely responsible for implementing Upgrades that require user configuration, installation or deployment; and

“**Workaround**” or “**Temporary Fix**” means a change advised by SmartCom in the procedures to be followed by Buyer to avoid an Error without significantly impairing performance of the SaaS Services.

## Additional Terms

1. Buyer requests and SmartCom agrees to provide Support for the License Term. SmartCom’s obligations under this Schedule No. 1 (Support) only apply during the License Term.
2. Support is only available in the English language and is provided solely at the Website, via email or telephone or in any combination thereof.
3. SmartCom will log all Errors with the SaaS Services reported by Buyer in accordance with the procedure set out this Schedule No. 1 (Support). Upon identification of any Error, Buyer shall provide SmartCom with enough information to reproduce the Error. If SmartCom is unable to reproduce the Error, SmartCom will request a second sample. If SmartCom is still unable to reproduce the Error from this second sample, then SmartCom will close the reported Error. SmartCom will notify Buyer as soon as possible if it determines that no Error exists or if SmartCom is unable to reproduce the reported Error. All Resolutions shall only be implemented during planned downtime which is normally outside of Office Hours. Buyer shall only submit non-production data (and excluding any Personal Data intended for submission from Buyer systems to the SaaS Services) to SmartCom pursuant to this Schedule No. 1 (Support). SmartCom accepts no responsibility or liability for any other data provided to SmartCom pursuant to this Schedule No. 1 (Support).
4. SmartCom shall use all reasonable efforts to respond to an Error within the Response Time and resolve the Error within the Resolution Time, in each case commensurate with the Error Severity Levels as determined by SmartCom. However, SmartCom does not guarantee that it will be able to resolve all Errors and if the prescribed Resolution Time expires before the first available planned downtime, the Resolution Time shall automatically be extended to the next available planned downtime.
5. Support does not include any training services and the offering of any such services shall be at the sole option of SmartCom and subject to additional Charges to be agreed separately for each such situation.
6. The provision of Support is contingent on Buyer’s compliance with the following additional obligations: (i) Buyer’s personnel shall be trained in use of the SaaS Services; (ii) Buyer shall provide SmartCom with sufficient documentation, data, details and assistance with respect to any reported Errors so as to enable SmartCom to reproduce and verify the same as an Error; (iii) Buyer shall assist SmartCom to diagnose and correct reported Errors by providing: (a) all relevant documentation and records, including sample output and other diagnostic information; and (b) interaction with personnel who have authority to implement remedial actions as instructed by SmartCom.

Buyer acknowledges that failure to provide such assistance will affect SmartCom's ability to meet a Response Time and or Resolution Time.

7. SmartCom shall have no obligation to provide Support in connection with any Error, questions or problems that arise from: (i) use of the SaaS Services in a manner other than described in the User Guide; (ii) the negligence or intentional misconduct of any User; (iii) failure by Buyer to implement reasonable recommendations in respect of or solutions to Errors previously advised by SmartCom; (iv) the creation or correction of C# or .NET code, Java, JavaScript, XSL/XSL:FO templates, or API integration issues; or (v) internet service provider failures.
8. Provision of Support as described in this Schedule No. 1 (Support) is SmartCom's sole obligation, and Buyer's sole remedy, with respect to the Support of the SaaS Services. SmartCom shall have no other liability or obligation to Buyer with respect to any Errors or other real or perceived problems with the SaaS Services.

## Error Severity Levels

The table below shows the Response Times in respect of the Error Severity Levels:

ERROR SEVERITY LEVEL	SERVICE LEVELS	
	RESPONSE TIME (within)	RESOLUTION TIME (within)
S1	1 Hour	48 Hours
S2	2 Hours	10 Days
S3	8 Office Hours	30 Working Days
S4	5 Working Days	Future Release
S5	10 Working Days	Future Release

## Schedule No. 2 (Data Protection & Privacy)

In respect of the Customer Data (to the extent it comprises Personal Data), SmartCom acts as a processor.

### 1. Definitions and Interpretation

1.1 In addition to the terms defined in Section 1 of the MSA, unless the context otherwise requires:

**"DP Regulator"** means any person or regulatory body with responsibility for monitoring and/or enforcing compliance with the Privacy Laws;

**"Privacy Laws"** means any laws and regulations in relating to privacy or the use or processing of data relating to natural persons to the extent they apply to a particular Party, including: (a) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (b) EU Regulation 2016/679 ("**GDPR**"); (c) General Data Protection Regulation ((EU) 2016/679) as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (d) the Data Protection Act 2018; and (e) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR.

1.2 In this MSA, **"Data Subject"**, **"Personal Data"**, **"process"**, **"processing"**, **"processor"**, **"transfer"** (in the context of Personal Data transfers) and **"appropriate technical and organizational measures"** shall be interpreted in accordance with the applicable Privacy Laws.

### 2. Data Protection

2.1 In relation to the performance of its obligations under this MSA, each Party shall comply with the provisions imposed on them by the Privacy Laws. Where Customer transfers Personal Data to SmartCom, whether as part of the Services or otherwise, Customer warrants to SmartCom that it has the right to transfer such Personal Data to SmartCom, and that it has secured a lawful data processing ground, in accordance with and in compliance with applicable Privacy Laws, to process such Personal Data and to share such Personal Data with SmartCom.

2.2 Each Party shall maintain records of all processing operations relating to this MSA under its responsibility that contain at least the minimum information required by the Privacy Laws and shall make such information available to any DP Regulator on request.

2.3 Customer confirms that Appendix 1 to this Schedule No. 2. (Data Protection & Privacy) sets out details of the processing of Personal Data to be undertaken by SmartCom in connection with this MSA, the types of Personal Data, categories of Data Subjects, and nature and purposes of processing. Such processing shall take place throughout the duration of this MSA and/or an applicable Order. Customer shall be solely responsible for ensuring the continued accuracy of the particulars contained in Appendix 1.

### 2.4 SmartCom as a processor

To the extent that SmartCom processes any Personal Data on behalf of Customer pursuant to this MSA as a processor, SmartCom shall:

- (a) process such Personal Data only in accordance with Customer's written instructions from time to time (including those set out in this MSA) save for processing which SmartCom is required to do pursuant to any Applicable Law;
- (b) take reasonable steps to ensure that any personnel who have access to such Personal Data are subject to binding obligations of confidentiality when processing such Personal Data;
- (c) implement and maintain technical and organizational measures and procedures to ensure an appropriate level of security for such Personal Data, including protecting such Personal Data against the risks of accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, dissemination or access;
- (d) inform Customer if any such Personal Data is (while within SmartCom's possession or control) subject to a personal data breach (as defined in Article 4 of GDPR) without undue delay after becoming aware, and provide the following information:
  - i) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records;
  - ii) communicate the name and contact details of the DPO or other contract point where more information can be obtained;
  - iii) describe the likely consequences of the personal data breach; and
  - iv) describe the measures taken or proposed to be taken by SmartCom to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
- (e) not disclose any such Personal Data to any Data Subject or to a Third Party other than at the written request of Customer, or in order to comply with a requirement of a DP Regulator, or as expressly provided for in this MSA;
- (f) at the written request of Customer, return or delete all such Personal Data on termination or expiry of this MSA, and/or an applicable Order, and not make any further use of such Personal Data (except to the extent that continued processing of any such Personal Data is required by SmartCom; or is required to be retained under Applicable Law. For the avoidance of doubt, SmartCom shall not retain any Customer Data;
- (g) provide to Customer and any DP Regulator (at Customer's cost and at SmartCom's then time and material rates) all information and assistance necessary to demonstrate or ensure compliance with the obligations in this Section 2.4;
- (h) no more than once every calendar year and subject to SmartCom having the right to do so, permit Customer or its representatives (at Customer's cost at SmartCom's then time and material rates) to access any relevant premises, personnel or records of SmartCom on reasonable notice (but being no less than fifteen (15) Working Days) to audit and otherwise verify compliance with this Section 2.4);
- (i) take such steps as are reasonably required to assist Customer (at Customer's cost at SmartCom's then time and material rates) in ensuring compliance with Customer's obligations under Articles 30 to 36 (inclusive) of the GDPR as they relate to SmartCom's obligations under this MSA;

- (j) to the extent feasible based upon the nature of processing conducted by SmartCom, notify Customer within seven (7) Working Days if it receives a request from a Data Subject to exercise its rights under the Privacy Laws in relation to that person's Personal Data; and
  - (k) to the extent feasible based upon the nature of processing conducted by SmartCom, provide Customer with its reasonable co-operation and assistance in relation to any request made by a Data Subject to exercise its rights under the Privacy Laws in relation to that person's Personal Data. SmartCom shall not charge for such requests unless such request is manifestly unjust or excessive, in which case SmartCom shall reserve the right to charge Customer a reasonable administration fee.
- 2.5 In the course of SmartCom acting as processor, if either Party receives any complaint, notice or communication which relates directly or indirectly to the processing of Personal Data by the other Party or to either Party's compliance with the Privacy Laws, it shall promptly notify the other Party and it shall provide the other Party with reasonable co-operation and assistance in relation to any such complaint, notice or communication.
- 2.6 Subject to Sections 2.7 to 2.11 (inclusive) below, SmartCom may appoint subprocessors of Personal Data on behalf of Customer. SmartCom shall procure that any such subprocessors enter into a written contract with SmartCom which contains obligations for the protection of Personal Data which are no less onerous than those set out in this Schedule No. 2 (Data Protection & Privacy). For the avoidance of doubt, SmartCom shall not appoint a subprocessor of Customer Data without Customer's written consent.
- 2.7 SmartCom's current list of subprocessors ("**Current Subprocessors**") which are used to undertake processing of Personal Data on behalf of Customer is accessible online at the Community Page. By entering into this MSA, Customer approves the use of the Current Subprocessors to the extent that they are used in providing the Services. The rights afforded to Customer in Sections 2.8, 2.9 and 2.10 of this Schedule No. 2 (Data Protection & Privacy) shall not apply in relation to Current Subprocessors.
- 2.8 Following the date of this MSA, SmartCom shall provide published updates via the Community Page in accordance with Section 2.4 of the MSA (notwithstanding any notice clauses set out in this MSA) of its intended appointment of a new subprocessor.
- 2.9 If Customer wishes to object to SmartCom's use of such subprocessor in accordance with and pursuant to Section 2.8 of this Schedule No. 2 (Data Protection & Privacy):
  - (a) Customer must notify SmartCom in writing within ten (10) Working Days of the notification from SmartCom; and
  - (b) Customer's objection to the relevant appointment must be on the basis that the relevant appointment would result in a breach of Customer's ability to comply with its obligations under Privacy Laws as a result of the relevant appointment.
- 2.10 If Customer validly objects to any new subprocessor in accordance with Section 2.9 of this Schedule No. 2 (Data Protection & Privacy), SmartCom will use reasonable efforts to make available to Customer an alternative solution or arrangement to avoid the processing by the relevant subprocessor of any Personal Data provided by Customer, provided that:
  - (a) SmartCom shall not be required to implement an alternative solution or arrangement which unreasonably burdens SmartCom; and
  - (b) SmartCom shall be entitled to make a reasonable additional charge to cover the costs of implementing and operating the alternative solution or arrangement.
- 2.11 If SmartCom is unable to make available an alternative solution or arrangement within a reasonable period of time (which shall not exceed ninety (90) days) or if Customer is unwilling to pay any charge by SmartCom to cover the costs of implementing and operating the alternative solution or arrangement, Customer may, by written notice to SmartCom terminate the MSA and all Orders, in which case, Customer shall be entitled to receive a pro rata refund of any prepaid Annual Fees and other applicable charges for the period following the effective date of termination.

## Appendix 1 to Schedule No. 2 (Data Protection & Privacy) (Particulars of Processing)

The Personal Data processing activities carried out by SmartCom under this MSA and an applicable Order may be described as follows:

### Subject matter of processing

[Customer to provide a brief description of the subject matter of the processing, i.e.; the subject matter of the MSA as it involves Personal Data]

### Nature and purpose of processing

SmartCom will process Personal Data in order to administer and provide the Services, Support and Consultancy Services.

### Categories of Personal Data

Please select all of the categories of Personal Data which are subject to the processing:

<input type="checkbox"/>	Name and contact details	<input type="checkbox"/>	Demographic data (age, date of birth, gender, etc.)
<input type="checkbox"/>	Payment card data (e.g.; PCI)	<input type="checkbox"/>	Data about children
<input type="checkbox"/>	Racial/ethnic origin	<input type="checkbox"/>	Other financial data (e.g.; bank account details)
<input type="checkbox"/>	Trade Union Membership	<input type="checkbox"/>	IT system information (e.g.; user ID)
<input type="checkbox"/>	Physical or mental health	<input type="checkbox"/>	Email content and transmission data
<input type="checkbox"/>	Sex life/sexual orientation	<input type="checkbox"/>	Details of goods or services provided to or for the benefit of individuals
<input type="checkbox"/>	Biometric/genetic data	<input type="checkbox"/>	Religious or philosophical beliefs
<input type="checkbox"/>	Employment details		
<input type="checkbox"/>	Other, please specify:		

### Categories of data subjects

Insert the categories of data subjects (i.e.; individuals) whose data is subject to the processing. Please select all of the categories of data subjects who are subject to the processing:

<input type="checkbox"/>	Customer Employees	<input type="checkbox"/>	Customer's clients
<input type="checkbox"/>	Former Customer Employees	<input type="checkbox"/>	Prospective clients
<input type="checkbox"/>	Complainants, correspondents and enquirers		
<input type="checkbox"/>	Past, present and prospective advisors, brokers, consultants, suppliers, contractors, subcontractors and agents		
<input type="checkbox"/>	Other, please specify:		



## Schedule No. 3 (Security)

SmartCom has implemented and will maintain and enforce this security policy (this "**Security Policy**") in respect of the SaaS Services, which includes reasonable and appropriate technical, administrative, physical and other security measures to protect against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data while such Data is in SmartCom's possession or under its control.

The Security Policy applies to each of SmartCom's hosting deployments, namely:

1. SmartCom's co-location hosted deployment;
2. AWS deployment; and
3. the Appliance (as defined in an applicable Order).

Where Buyer elects for an Appliance deployment, SmartCom does not have access to a Buyer's electronic data or information (including any Personal Data therein) submitted by Buyer or User to the SaaS Services (for SmartCOMM typically to be combined with Buyer's templates to produce individualized output files) ("**Transaction Data**") and therefore does not process such data. Where an Appliance deployment is used, Buyer maintains control over its Transaction Data within its own systems and environments to which SmartCom does not have access. SmartCom will perform the SaaS Services under an Appliance deployment without access to Transaction Data.

The Security Policy comprises the following topics, in line with Industry Standards:

1. Governance and Program Management
2. Physical and Environmental Security
3. Systems Access Controls & Monitoring
4. Asset Management
5. Encryption requirements
6. Software Development Security
7. Security Patches
8. Vulnerability Management and Testing
9. Security Training
10. Data Breach
11. Subcontractors
12. Background Checks
13. Business Continuity
14. Certifications
15. Audit

SmartCom will review, and if necessary, update the Security Policy in line with good industry practice at least annually.

For the purposes of this Schedule No. 3 (Security), "**Industry Standards**" shall mean commonly accepted information security best practices for service providers providing technology services.

### 1. **Governance and Program Management**

- a) The Security Policy will comply with ISO/IEC 27001 and be consistent with Industry Standards.
- b) SmartCom will designate an individual who is responsible for the implementation, maintenance and enforcement of the Security Policy.

### 2. **Physical and Environmental Security**

- a) SmartCom will ensure appropriate security controls for all physical entry points to locations containing systems that host the SaaS Services (each a "**Site**"), including the following:
  - i) access to Sites by authorized personnel will be controlled and restricted by use of appropriate security barriers, security cameras, entry controls and authentication controls;
  - ii) electronic and written access logs will be maintained for a minimum period of thirty (30) days;
  - iii) all personnel will be required to wear some form of visible identification;
  - iv) SmartCom maintains a clear desk and clear screen policy at SmartCom premises and in respect of SmartCom Users (as defined in Section 3, below);
  - v) visitors without access-rights to a Site will be escorted at all times by authorized personnel;
  - vi) SmartCom shall provide the SaaS Services from Sites that are physically separated from each other for the purposes of separation of essential hardware; and

- vii) where feasible and permitted by Applicable Law, CCTV cameras will be installed and monitored 24/7, with such recordings retained for at least thirty (30) days.
- b) SmartCom will ensure that equipment used to provide the SaaS Services will be protected from power failures and other disruptions caused by failures in supporting utilities (see Section 13, below).

**3. Systems Access Controls & Monitoring.** The following security controls, procedures and practices will apply to SaaS Services and/or the SmartCom Technology used to provide the SaaS Services:

- a) **Logical Security.** To protect against unauthorized access to the SaaS Services, SmartCom will:
  - i) employ a formal procedure for granting and revoking access and access rights to SmartCom employees and/or contractors (each a "SmartCom **User**") to the SmartCom Technology used to provide the SaaS Services;
  - ii) follow a separation of duties standard and develop a formal approval process and audit trail for all access requests;
  - iii) review each SmartCom User's access rights to confirm they are appropriate for their role;
  - iv) create security practices and controls regarding the selection and use of strong passwords. Such password controls will include minimum length, two-factor authentication, alpha/numeric characters, lockouts, expirations, stored encrypted and password reuse;
  - v) employ idle-lock for unattended equipment to prohibit access and use by unauthorized individuals;
  - vi) control access to operating systems through a secure log-on procedure;
  - vii) provide information processing system users with a unique identifier ("**User ID**");
  - viii) control the use of utility programs that are capable of overriding system and application controls; and
  - ix) close inactive application sessions, when technically possible, after a defined period of inactivity.
- b) **Network Access Control.** SmartCom will employ the following network access controls with respect to internal, external and public network services that allow access to the SmartCom Technology used to provide the SaaS Services:
  - i) Industry Standards authentication mechanisms for network users and equipment;
  - ii) electronic perimeter controls (including firewalls) that protect the SaaS Services from unauthorized logical access;
  - iii) authentication methods to control access by remote users and two-factor authentication; and
  - iv) logical access control for diagnostic and configuration ports.
- c) **User ID.** SmartCom will assign a User ID to all SmartCom Users accessing the SmartCom Technology. User ID authentication will be required before any access to SmartCom Technology is granted to a SmartCom User.
- d) **Removal of Access Rights.** The access rights of SmartCom Users to the SmartCom Technology will be removed within twenty-four (24) hours upon termination of their employment, contract or agreement or adjusted upon a change in their duties.
- e) **Minimum Access Rights.** SmartCom will provide SmartCom Users with the minimum access rights and privileges to the SmartCom Technology needed to perform a particular function or transaction. SmartCom User access reviews will be conducted at least annually and updated as necessary.
- f) **Systems Monitoring.** SmartCom will employ multiple levels of system monitoring including server fault monitoring, service functionality monitoring, API functionality monitoring, user functionality monitoring and service availability monitoring.
- g) **Security Monitoring.** SmartCom will employ Industry Standards in respect of security configuration and 24x7 security monitoring, including the use of in-house and specialist third-party security operations services.

**4. Asset Management**

- a) SmartCom will implement rules for the acceptable use of Data and assets which comply with Industry Standards.
- b) SmartCom prohibits SmartCom Users from storing Data on portable devices or media. SmartCom Users may, however, store data (which excludes Personal Data or Buyers' end user data) uploaded by the Buyer or User to the content management system which forms the basis for the Buyer (i) configuration of templates, styles, layouts and related resources; and/or (ii) projects and their associated resources ("**CMS Data**") on laptops with full-disk encryption provided there is a business purpose that requires such storage such as for Support or Consultancy Services. SmartCom shall delete such CMS Data when the business purpose no longer exists.
- c) Where applicable in respect of SmartCom's co-location hosting equipment, SmartCom will implement an inventory management program and perform monitoring to control the installation and movement of hardware, software and communication equipment used to provide the SaaS Services.
- d) All media and assets that contain Data leaving SmartCom's custody shall be encrypted, sanitized, destroyed, or purged of Data in accordance with Industry Standards to ensure that Data has been deleted, and is not easily recoverable, prior to leaving SmartCom's custody. Sanitization refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed, according to the guidelines of the Department of Defense 5220-22M standard.
- e) SmartCom will prohibit employees from storing Data on personally owned equipment.

**5. Encryption Requirements**

- a) All specific Transaction Data uploaded to the SaaS Services in respect of a specific communication generated by the SaaS Services shall be encrypted over public networks in transit to accepted Industry Standards of not less than TLS 1.2, using frequently strong cipher suites, as applicable.
- b) Transaction Data stored in databases comprised within the SaaS Services shall be encrypted at rest to at least AES128 bit encryption.
- c) SmartCom shall maintain a key-management process for relevant encryption keys and store such keys in a purpose-built key management solution, each in line with Industry Standards.

#### 6. **Software Development Security**

SmartCom will maintain a software development lifecycle program that is based on Industry Standards, which includes the utilization of software for code scans for vulnerabilities and Viruses as well as periodic security reviews, access controls in respect of all proprietary source code and quality assurance testing prior to the release of any new software comprised in the SaaS Services.

#### 7. **Security Patches**

- a) SmartCom will implement security patches within a prudent timeframe as determined by SmartCom. Particular consideration is given to:
  - i) the severity of any identified security vulnerability;
  - ii) the extent to which a vulnerability may affect any specific system or sub-system;
  - iii) the extent to which a system may be insulated from particular attack vectors; and
  - iv) a holistic consideration of the security implications that could arise in respect of the introduction of a particular security patch.
- b) Furthermore, SmartCom documents and records all material considerations and identified issues in respect of any security patches.

#### 8. **Vulnerability Management and Testing**

- a) SmartCom shall arrange for a suitably-qualified, independent Third Party ("**External Tester**") to conduct penetration testing of the SaaS Services at least once in any twelve (12) month period. Subject to sub-sections (i) and (ii) below, penetration testing must include all tests which, in the reasonable opinion of SmartCom, a hacker may use to attack the SaaS Services, including attacks aimed at disrupting, damaging or changing the SaaS Services ("**Penetration Testing**"). SmartCom must ensure in relation to this Section 8:
  - i) the External Tester will take all reasonable precautions to avoid damaging the SaaS Services and will not download any Data from the SaaS Services;
  - ii) the External Tester will ensure that any Penetration Testing has minimal or no disruption to the SaaS Services; and
  - iii) after conducting each round of Penetration Testing, the External Tester must provide a written report on the results of the Penetration Testing to SmartCom. SmartCom will subsequently share redacted results of the Penetration Testing with Buyer.
- b) SmartCom shall scan the SaaS Services for known vulnerabilities periodically (each a "**Vulnerability Scan**").
- c) SmartCom must remediate any material deficiencies in the security of the SaaS Services identified by the External Tester from the Penetration Testing and/or Vulnerability Scan within a reasonable timeframe.

#### 9. **Security Training**

All SmartCom Users involved in the provision of the SaaS Services will receive training in respect of data privacy/data protection; confidentiality and measures to protect Confidential Information; and security training in line with Industry Standards on an annual basis regarding the appropriate protection of Data. Mandatory security training occurs for all new SmartCom Users and annually thereafter, and is documented and monitored.

#### 10. **Data Breach**

- a) SmartCom will maintain a data breach response and crisis communication program that is reasonably designed to detect, contain, respond and recover from a Data Breach.
- b) If SmartCom becomes aware of a Data Breach, SmartCom will:
  - i) notify Buyer without undue delay in respect of a Data Breach;
  - ii) take steps to minimize the Data Breach;
  - iii) take appropriate measures to secure the Personal Data and prevent a recurrence of the Data Breach;
  - iv) provide reasonable information to Buyer about its remediation efforts and make any applicable notifications to a regulator; and
  - v) to the extent available to SmartCom, provide Buyer with reasonable details of the Data Breach, including, description of the Personal Data subject to the Data Breach and date and time of the Data Breach.
- c) SmartCom will take appropriate steps to remediate the root cause(s) of a Data Breach and will provide Buyer with a summary of the results of the investigation and any remediation efforts taken by SmartCom.

#### 11. **Subcontractors**

In respect of those subcontractors that have access to Data, SmartCom will maintain a risk management program focused on the identification, evaluation and validation of a subcontractor's privacy, security and business continuity controls to ensure that the subcontractor utilizes appropriate controls as applicable to the services delivered by such subcontractor. SmartCom will review and assess the security policies and practices of such subcontractors to attest and ensure applicable controls are in place with respect to Data.

## 12. Background Checks

- a) To the extent permitted by Applicable Law, SmartCom will, at its expense, conduct a background check on each employee that is involved in the provision of the SaaS Services to Buyer under this Addendum. The background investigation will be performed at the time an employee is offered employment by SmartCom and will include the following:
  - i) Social Security Number trace and validation;
  - ii) Criminal felony and misdemeanor search for previous seven (7) years for every county identified by the Social Security Number trace;
  - iii) Widescreen plus national criminal search;
  - iv) Federal criminal search for the current district of residence;
  - v) Employment history for the previous five (5) years;
  - vi) Education report for the highest degree achieved;
  - vii) Credit report check; and
  - viii) Global sanctions and enforcement check.
- b) SmartCom will conduct an inquiry into any personnel who participate in the provision of the SaaS Services who has received a negative background investigation and SmartCom will not permit such personnel whose investigation reveals a risk to participate in the provision of the SaaS Services, access to SmartCom Technology or SmartCom source code.
- c) Upon Buyer's written request, SmartCom will certify that SmartCom is in compliance with this Section 12.

## 13. Business Continuity

- a) SmartCom will have in place and maintain a formalized business continuity and disaster recovery plan (the "**Plan**") which will reasonably enable SmartCom to recover from an incident or event whether natural or manmade which prevents SmartCom from providing access to the SaaS Services ("**Disaster**") and continue providing the SaaS Services as set forth in this Addendum and/or an applicable Order.
- b) The Plan will be documented in written form and will include details appropriate for the SaaS Services, the complexity of the environment and probability of occurrence, including:
  - i) a description of the facilities, employees, roles, responsibilities, procedures and processes required to provide a coordinated approach to managing Disaster response activities at the time of any Disaster;
  - ii) actions to be taken before, during and after SmartCom's reasonable determination that an incident or event is a Disaster ("**Disaster Declaration**"); and
  - iii) the recovery time objective and recovery point objective for the SaaS Services.
- c) SmartCom will designate employees to lead the implementation of the Plan and such person(s) will appoint response and recovery teams who will execute the procedures described in the Plan.
- d) SmartCom will have and maintain at least one alternative data center or AWS Availability Zone that is separate and apart from its primary data center /AWS Availability Zone and meets the following requirements:
  - i) the alternative must have functional capability and capacity sufficient to assume the production responsibilities and capacities of the primary;
  - ii) the alternative will be located at a reasonable distance from the primary and will be supplied by utilities (e.g., communication, power) from different sources than those supplying the primary so as to minimize the likelihood that both would be affected by the same Disaster; and
  - iii) the alternative will have security features that are no less stringent than those of the primary.
- e) SmartCom will review and, if necessary, update the Plan at least once annually.
- f) Upon Buyer's written request but not more than once in any twelve (12) month period, SmartCom will provide Buyer with the table of contents for the Plan and/or arrange a meeting (either in person or via an online meeting service) to review and Plan with Buyer.
- g) SmartCom will execute planned annual tests of the Plan to ensure the Plan is effective and fully operational in respect of the SaaS Services (the "**Annual Plan Test**").
- h) Upon Buyer's written request, but not more than once in any twelve (12) month period, SmartCom will provide Buyer with the redacted results of the applicable Annual Plan Test.
- i) Upon Disaster Declaration, SmartCom will implement the Plan to restore the SaaS Services in accordance with the specifications set forth in the Plan.

- j) SmartCom will utilize its Community Page, or such other communication method available to SmartCom during the Disaster, to notify Buyer of a Disaster Declaration and activation of the Plan and will use reasonable efforts to provide status updates.
- k) The Plan will require SmartCom to backup, archive, and maintain duplicated or redundant systems that shall have the ability to fully recover the platform and all data within the following timeframes:
  - i) Recovery Time Objective (“RTO”) – SmartCom has four (4) hours from Disaster Declaration to commence and complete cut over of the SaaS Services to its alternative data center.
  - ii) Recovery Point Objective (“RPO”) – RPO for the SaaS Services is one (1) hour.

#### 14. Certifications

SmartCom shall, at its sole cost: (a) have a nationally-recognized accounting firm conduct an audit in accordance with the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) developed by the American Institute of Certified Public Accountants, and have such accounting firm issue a Service Organization Control 1 (SOC-1) Type 2 report and a Service Organization Control 2 (SOC-2) Type 2 report (or substantially similar reports in the event that the SSAE 18 auditing standard SOC-1 Type 2 and/or SOC-2 Type 2 reports is/are no longer an industry standard) which shall cover the environment maintained by SmartCom to provide the SaaS Services; and (b) upon request by Buyer, provide Buyer and its independent auditors with a copy of the SOC-1 Type 2 and SOC-2 Type 2 reports, together with plans for addressing any deficiencies identified in the report(s). Company shall also provide Buyer and independent auditors, upon request, with the results of any other independent audits conducted from time to time with respect to Company's environment for providing the SaaS Services, information security measures, and/or its software development techniques, practices or methodologies.

#### 15. Audit

- a) Buyer and/or its duly authorized representatives shall have the right to review, no more than once in any twelve (12) month period and subject to the provision of at least fifteen (15) Working Days' notice, SmartCom's compliance with this Security Policy (a “**Security Policy Audit**”). Should Buyer request a Security Policy Audit, then SmartCom shall allow Buyer to inspect SmartCom premises, systems and appropriate records to demonstrate SmartCom 's compliance with the Security Policy. Wherever possible, SmartCom shall also provide copies of audit reports of third-party hosting providers (including AWS where applicable) to Buyer demonstrating such parties' compliance with their security standards. A Security Policy Audit shall take place during normal business hours to reasonably limit disruption to SmartCom's business. Any Security Policy Audit shall be subject to the following limitations:
  - i) the use of any third-party auditor shall be subject to SmartCom's prior written approval (and the execution of appropriate confidentiality terms), such approval not to be unreasonably withheld or delayed;
  - ii) Buyer or any auditor conducting any such audit shall at all times comply with any and all reasonable security and confidentiality guidelines and other policies of SmartCom with respect to the audit; and
  - iii) provision by SmartCom of personnel to assist with any Security Policy Audit shall be restricted to fifteen (15) man-hours in respect of each Security Policy Audit, after which further assistance shall be chargeable at SmartCom's then prevailing time and materials rates for Consultancy Services.
- b) Buyer agrees that SmartCom will have the right to reasonably redact or deny access to any records, data, documentation systems, equipment, software and documentation requested during an audit if it contains the Confidential Information of its other customers or would cause SmartCom to be in breach of its security policies or other contractual obligations.

## Schedule No. 4 (Service Levels)

### Availability Service Level Agreement

1. Availability shall be calculated on a monthly basis as set out in this Schedule No. 4 (Service Levels).
2. In addition to the terms defined in Section 1 of the Addendum the following terms shall have the following meanings:

**Availability** means availability of the SaaS Services which shall be calculated using the following formula:

$$\frac{A-B}{A} \times 100 = \text{Availability Service Level Percentage}$$

where:

- A** = The total aggregate number of minutes in the relevant calendar month LESS the total aggregate number of minutes of Exclusions.  
**B** = The total aggregate number of minutes of downtime (excluding downtime caused by Exclusions) during the relevant month.

**Exclusions** means (i) planned downtime during the relevant month (ii) any unavailability caused by circumstances beyond SmartCom's reasonable control (including as a result of Force Majeure; and (if applicable in accordance with a Usage Policy attached to an Order), unavailability of the Appliance; and/or unavailability of the Appliance Hardware) (where Appliance and Appliance Hardware are defined in an applicable Usage Policy).

**Monthly Period** means the calendar month in respect of which the Availability Service Level Percentage has been calculated.

**Monthly Fees** means the portion of the Annual Fees attributable to a Monthly Period and shall be calculated as one twelfth (1/12) of the Annual Fees.

**Service Credit** means the percentage of the Monthly Fees to be credited to Buyer by SmartCom upon failure to achieve a 99.5% Availability Service Level Percentage as set out in the table in Section 4 of this Schedule No. 4 (Service Levels).

3. Where the Availability Service Level Percentage falls below 99.5%, Buyer shall be entitled to a Service Credit at the rate specified in the table below provided that such request is notified to SmartCom within sixty (60) days of the end of the Monthly Period for which a Service Credit accrues.

4. Buyer's sole financial remedy in relation to SmartCom's failure to meet the Availability Service Level Percentages shall be as set out in this Schedule No. 4 (Service Levels) and Buyer shall have no right to recover additional damages in respect of such failure. In no event shall the total amount of Service Credits issued to Buyer in a twelve (12) month period exceed 10% of the Annual Fees paid and payable by Buyer for that period. Service Credits shall be applied as a credit against any amounts payable (and not yet paid) by Buyer to SmartCom. Where no amount is payable by Buyer, SmartCom will promptly refund to Buyer an amount equivalent to the Service Credit applicable. In addition to the financial remedy described above, should the Availability Service Level Percentage fall below 99.5% in any three (3) consecutive months ("**Persistent Service Failure**"), then Buyer, not later than sixty (60) days after the occurrence of the Persistent Service Failure, shall be entitled to terminate the applicable Order (without further liability attributable to SmartCom) by providing written notice to SmartCom to such effect.

Availability Service Level Percentage (%)	Service Credit (% of Monthly Fees)
99.5 and above	None
Between 99.4 and 99.49	5%
Between 99.3 and 99.39	6%
Between 99.2 and 99.29	7%
Between 99.1 and 99.19	8%
Between 99.0 and 99.09	9%
Less than 99.0	10%

By way of example only, if Buyer's Annual Fees are \$100,000 and the Availability Service Level Percentage for a Monthly Period is 99.4%, Buyer will receive a Service Credit for £416.67 ([£100,000/12 months] x 0.05).

## Annex 1: Usage Policy (SmartCOMM AWS)

This Usage Policy contains the limitations on Buyer's use of the SaaS Services and the consequences of exceeding those limitations.

### 1. Definitions

In addition to the terms defined in section 1 of the Addendum, the following terms shall have the following meanings:

"AWS"	means hosting of the SaaS Services on Amazon Web SaaS Services located in the UK ;
"Batch"	means groups of Output submitted to the SaaS Services on a batch basis via the batch APIs;
"File Storage"	means input files, output files and log files relating to Batch;
"Final Output"	means Output generated by the SaaS Services that is no longer editable via the SaaS Services and may be issued by Buyer to third parties;
"Generated Document"	means Final Output generated by the SaaS Services from a single template design in a single output format;
"Interactive Page"	means a Page which can be only edited by Buyer using the SaaS Services prior to it being Final Output;
"Interim Output"	means any Output except Final Output;
"Non-Interactive Page" or "On-Demand Page"	means a Page which once created by Buyer using the SaaS Services cannot be further edited;
"Order Year"	means each twelve (12) month consecutive period beginning from the commencement of the License Term;
"Output"	means a Page created through Buyer's use of the SaaS Services;
"Overage Unit"	means blocks of 10 Users or 1 million Pages;
"Page"	means each: (i) physical page face/side (or electronic equivalent) conforming to ISO 216 or ANSI/ASME Y14.1 generated or recorded Remotely or (ii) an email, SMS, or XML file generated or recorded Remotely;
"Page Allowance"	means the number of Pages which Buyer is authorized to process in an Order Year in consideration of the Annual Fee, all being specified or otherwise referred to in an Order;
"Remote" or "Remotely"	means location of SmartCom owned or controlled infrastructure upon which the SmartCom Technology operates; and
"Storage Allowance"	means the space as specified in an Order which is available on SmartCom's systems for storage of Data.

### 2. Smart Communications

#### 2.1. Page Allowance

Buyer's Page Allowance is stated in the Order. If it is exceeded in any Order Year, SmartCom may charge Overages at a premium of 50% above the list price stated in the Order for sufficient Overage Units to cover the excess Volume. If list price is not stated in the Order, then SmartCom's list price, current at the time of the Overage, shall apply as the basis for the list price.

If during any Order Year the average number of kilobytes per Page comprising the Final Output exceeds 100, then the applicable Volumes shall be deemed to be the number of Pages multiplied by the average number of kilobytes per Page and divided by 100.

#### 2.2. Storage Allowance

Buyer's Storage Allowance is 1GB per Tenancy. Additional storage usage will be charged at GBP600/GB/Order Year.

#### 2.3. Peak Allowance

Buyer is permitted to process up to 200 Pages per minute for each million Pages of Page Allowance. For example, if the Page Allowance is 10 million Pages, then up to 2,000 Pages per minute are permitted.

Maximum concurrent requests are 1 per million Remote Pages of Page Allowance.

If Buyer exceeds the above limits by 100% on any single occasion, or on three or more occasions in a calendar month, SmartCom reserves the right to restrict Buyer's throughput to levels set forth herein.

#### 2.4 Interim Output

Non-finalized Interactive Pages are the total number of Interactive Pages that have been created but are not Final Output. At the end of each Order Year, non-finalized Interactive Pages will be deemed Final Output for the purpose of calculating whether the total number of Interactive Pages are within the Page Allowance.

### **2.5 Migration Studio**

Each Page processed by Migration Studio shall be deemed to be a Remote Non-Interactive Page for the purposes of determining if the Volumes exceed the Page Allowance. SmartCom reserves the right to restrict usage of Migration Studio to not more than 5,000 Pages in any twenty-four (24) hour period.

### **3. Prohibitions**

If at any time Buyer contravenes any of the prohibitions listed in Section 3.2 of the Addendum, SmartCom may in its sole discretion suspend Buyer and/or User access to the SaaS Services, and may where possible, provide Buyer with notice of such suspension. SmartCom may further treat a contravention of Section 3.2 as an irremediable and material breach, entitling SmartCom to terminate the Addendum and Order with immediate effect.

## Schedule 5

### STANDARD CONTRACT FOR AWS MARKETPLACE

Standard Contract for AWS Marketplace - 2022 Update (2022-07-14)

#### 1. Scope.

**1.1 Terms and Conditions.** This Standard Contract for AWS Marketplace (the “**Standard Contract**”) sets forth the terms and conditions applicable to the licensing of Product from the licensor (“**Licensor**”) by the Party subscribing to the Product (“**Buyer**”), whether deployed into Buyer’s Computing Environment and/or made available as SaaS Service from Licensor’s Computing Environment. This Standard Contract only applies if the Product is expressly offered pursuant to the Standard Contract. The offer of Product pursuant to this , and Buyer’s purchase of the corresponding Subscription, constitutes each Party’s respective acceptance of this Standard Contract and their entry into this Agreement (defined below). Unless defined elsewhere in this Standard Contract, terms in initial capital letters have the meanings set forth in Section 13. Buyer and Licensor may be referred to collectively as the “**Parties**” or individually as a “**Party**”.

**1.2 Product Subscription.** Licensor will fulfill the Subscription to Buyer. A Subscription, as described in the applicable Product Listing and the corresponding purchase transaction, may be for Product deployed in Buyer’s Computing Environment and/or Product deployed via SaaS Service through Licensor’s Computing Environment. The pricing and term (if not on demand) are set forth in the Product Listing. Additional information concerning the Product and included services that is included or referenced in the Product Listing is a part of the Product Listing; such information may include but is not limited to: intended geographic use of the Product, any technical requirements for use of the Product, Support Services (which may vary by geography), information regarding Open Source Software and description of Licensor’s security practices.

**1.3 Agreement.** Each Subscription is subject to and governed by this Standard Contract, the applicable Product Listing, the terms and conditions of the NDA (if any), the Privacy and Security Terms for SaaS Service Subscriptions, and any amendments to any of the foregoing as may be agreed upon by the Parties, which together constitute the agreement between Buyer and Licensor (the “**Agreement**”). Each Subscription is a separate agreement between Buyer and Licensor. In the event of any conflict between the terms and conditions of the various components of this Agreement, the following order of precedence will apply: (a) any amendment agreed upon by the parties; (b) the Privacy and Security Terms for SaaS Service Subscriptions; (c) the NDA (if any); (d) the Product Listing; and (e) this Standard Contract.

#### 2. Licenses.

##### 2.1 Licensed Materials.

**2.1.1** If the Subscription is for a Product, or includes a component of a Product, deployed in Buyer’s Computing Environment, Licensor hereby grants to Buyer during the term of the Subscription, subject to Section 2.1.3, a nonexclusive, worldwide (subject to Section 12.4), nontransferable (except in connection with an assignment permitted under Section 12.2), non-terminable (except as provided in Section 10) license under all Proprietary Rights in and to the Product, or the applicable Product component, to deploy, operate and use the Product in Buyer’s Computing Environment and to allow its Users to access and use the Product, or the applicable Product component, as so deployed, in accordance with the Product Listing and the usage purchased in the Subscription.

**2.1.2** If the Subscription is for a Product, or includes a Product component, deployed via SaaS Service, Licensor hereby grants to Buyer during the term of the Subscription, subject to Section 2.1.3, a nonexclusive, worldwide (subject to Section 12.4), nontransferable (except in connection with an assignment permitted under Section 12.2), non-terminable (except as provided in Section 10) license under all Proprietary Rights in and to the Product, or the applicable Product component, to access and use the Product via the SaaS Service and to allow its Users to access and use the Product, or the applicable Product component, and SaaS Service, in accordance with the Product Listing and the usage purchased in the Subscription.

**2.1.3** Buyer may use the Product only: in support of the internal operations of Buyer’s and its Affiliates’ business(es) or organization(s), in connection with Buyer’s and its Affiliates’ products and services (but, for clarity, not as a stand-alone product or service of Buyer or its Affiliates), and/or in connection with Buyer’s and its Affiliate’s interactions with Users.

**2.1.4** Buyer may make a reasonable number of copies of the Documentation as necessary to use such Product in accordance with the rights granted under this Agreement, provided that Buyer includes all proprietary legends and other notices on all copies. Licensor retains all rights not expressly granted to Buyer under this Agreement.

**2.2 Affiliates and Contractors.** With respect to Affiliates and Contractors that Buyer allows to use the Licensed Materials: (a) Buyer remains responsible for all obligations hereunder arising in connection with such Affiliate’s or Contractor’s use of the Licensed Materials; and (b) Buyer agrees to be directly liable for any act or omission by such Affiliate or Contractor to the same degree as if the act or omission were performed by Buyer such that a breach by an Affiliate or a Contractor of the provisions of this Agreement will be deemed to be a breach by Buyer. The performance of any act or omission under this Agreement by an Affiliate or a Contractor for, by or through Buyer will be deemed the act or omission of Buyer.

**2.3 Restrictions.** Except as specifically provided in this Agreement, Buyer and any other User of any Licensed Materials, in whole or in part, may not: (a) copy the Licensed Materials, in whole or in part; (b) distribute copies of Licensed Materials, in whole or in part, to any third party; (c) modify, adapt, translate, make alterations to or make derivative works based on Licensed Materials or any part thereof; (d) except as permitted by Law, decompile, reverse engineer, disassemble or otherwise attempt to derive source code, algorithms or the underlying structure of the Product; (e) use, rent, loan, sublicense, lease, distribute or attempt to grant other rights to any part of the Licensed Materials to third parties; (f) use the

Licensed Materials to act as a consultant, service bureau or application service provider; or (g) permit access of any kind to the Licensed Materials to any third party.

**2.4 Open Source Software.** Subject to the requirements of Section 5.1(d), Product may contain or be provided with Open Source Software. If Buyer's use of the Product subjects Buyer to the terms of any license governing the use of Open Source Software, then information identifying such Open Source Software and the applicable license shall be incorporated or referenced in the Product Listing or Documentation. The terms of this Agreement apply to Open Source Software (i) to the extent not prohibited by the license to which the Open Source Software is subject, including without limitation, warranties and indemnification, (ii) and except to the extent required by the license to which the Open Source Software is subject, in which case the terms of such license will apply in lieu of the terms of this Agreement with respect to such Open Source Software, including without limitation, any provisions governing attribution, access to source code, modification and reverse-engineering.

**2.5 No Additional Terms.** No shrink-wrap, click-acceptance or other terms and conditions outside this Agreement provided with any Licensed Materials or any part thereof ("**Additional Terms**") will be binding on Buyer or its Users, even if use of the Licensed Materials, or any part thereof, requires an affirmative "acceptance" of such Additional Terms before access to or use of the Licensed Materials, or any part thereof, is permitted. All such Additional Terms will be of no force or effect and will be deemed rejected by Buyer in their entirety. For clarity, the Product Listing and or Documentation are not Additional Terms subject to this Section.

**2.6 High-Risk Activities.** The Product is not designed or developed for use in high-risk, hazardous environments requiring fail-safe performance, including without limitation in the operation of nuclear facilities, aircraft navigation or control systems, air traffic control, or weapons systems, or any other application in which the failure of the Product could lead to severe physical or environmental damages ("**High Risk Activities**"). Buyer will not use the Product for High Risk Activities.

### **3. Services.**

**3.1 SaaS Service.** If Buyer is purchasing a SaaS Service Subscription, Licensor will provide the Product to Buyer as a SaaS Service in accordance with the Product Listing promptly following purchase of the Subscription and continuing until termination of the Subscription. Licensor will provide Buyer all license keys, access credentials and passwords necessary for access and use of the Product via the SaaS Service ("**Keys**") as set forth in the Product Listing.

**3.2 Support Services.** Licensor will make available to Buyer Documentation concerning the use and operation of the Product, and Licensor will provide Support Services to Buyer as described, incorporated or referenced in the Product Listing.

### **4. Proprietary Rights.**

**4.1 Licensed Materials.** Subject to the licenses granted herein, Licensor will retain all right, title and interest it may have in and to the Licensed Materials, including all Proprietary Rights therein. Nothing in this Agreement will be construed or interpreted as granting to Buyer any rights of ownership or any other proprietary rights in or to the Licensed Materials or any Proprietary Rights therein.

**4.2 Feedback.** Buyer may, at its option, provide suggestions, ideas, enhancement requests, recommendations or feedback regarding the Licensed Materials or Support Services ("**Feedback**"), provided however, that Feedback does not include any Proprietary Rights of Buyer or Buyer's Affiliates or any Buyer Data or Buyer Materials. Licensor may use and incorporate Feedback in Licensor's products and services without compensation or accounting to Buyer, provided that neither Licensor nor its use of the Feedback identifies Buyer as the source of such Feedback. Feedback is not confidential to Buyer. Buyer will have no obligation to provide Feedback, and all Feedback is provided by Buyer "as is" and without warranty of any kind.

### **5. Warranties.**

**5.1 Licensed Materials.** Licensor represents and warrants that: (a) for Subscriptions with Entitlement Pricing, in the case of Product, or a component of a Product, deployed in the Buyer's Computing Environment, the Product or component will conform, in all material respects, to the Documentation, for 30 days after Buyer's purchase of the Subscription or the term of the Subscription, whichever is shorter, and, in the case of Product, or a component of a Product, deployed as a SaaS Service, the Product will conform, in all material respects, to the Documentation during the term of the Subscription; (b) a Product, or a component of a Product, provisioned for deployment in the Buyer's Computing Environment will not contain any automatic shut-down, lockout, "time bomb" or similar mechanisms that could interfere with Buyer's exercise of its rights under this Agreement (for clarity, the foregoing does not prohibit license keys that expire at the end of the Subscription); (c) Licensor will use industry standard practices designed to detect and protect the Product against any viruses, "Trojan horses", "worms", spyware, adware or other harmful code designed or used for unauthorized access to or use, disclosure, modification or destruction of information within the Product or interference with or harm to the operation of the Product or any systems, networks or data, including as applicable scanning the Product for malware and other security vulnerabilities and with up to date scanning software or service prior to making the Product (including any Product provided through Support Services) available to Buyer, and for Product or a component of a Product deployed via SaaS Service, scanning the Product or component on a regular basis; and (d) the Product, and Buyer's use thereof as permitted under this Agreement, will not be subject to any license or other terms that require that any Buyer Data, Buyer Materials or any software, documentation, information or other materials integrated, networked or used by Buyer with the Product, in whole or in part, be disclosed or distributed in source code form, be licensed for the purpose of making derivative works, or be redistributable at no charge.

**5.2 Services.** Licensor represents and warrants that any Support Services will be performed in a professional manner with a level of care, skill and diligence performed by experienced and knowledgeable professionals in the performance of similar services and in accordance with the Product Listing and Documentation.

**5.3 Remedies.** If any Product or Service fails to conform to the foregoing warranties, Licensor promptly will, at its option and expense, correct the Product and re-perform the Services as necessary to conform to the warranties. If Licensor does not

correct the Product or re-perform the Services to conform to the warranties within a reasonable time, not to exceed 30 days (or such other period as may be agreed upon by the Parties) (the “**Cure Period**”), as Buyer’s sole remedy and Licensor’s exclusive liability (except as provided in Section 9), Buyer may for a period of 30 days following the conclusion of the Cure Period (or such other period as may be agreed upon by the Parties), elect to terminate the Subscription and this Agreement without further liability and Licensor will provide Buyer with a refund of any fees prepaid to Licensor by Buyer, prorated for the portion of the Subscription unused at the time Buyer reported the breach of warranty to Licensor, as well as, if applicable, any service credits available under Licensor’s Support Services or other policies.

**5.4 Warranty Exclusions.** Licensor will have no liability or obligation with respect to any warranty to the extent attributable to any: (a) use of the Product by Buyer in violation of this Agreement or applicable Law; (b) modifications to the Licensed Materials not provided by Licensor or its Personnel; (c) use of the Product in combination with third-party equipment or software not provided or made accessible by Licensor or contemplated by the Product Listing or Documentation; or (d) use by Buyer of Product in conflict with the Documentation, to the extent that such nonconformity would not have occurred absent such use or modification by Buyer.

**5.5 Compliance with Laws.** Each Party represents and warrants that it will comply with all applicable international, national, state and local laws, ordinances, rules, regulations and orders, as amended from time to time (“**Laws**”) applicable to such Party in its performance under this Agreement.

**5.6 Power and Authority.** Each Party represents and warrants that: (a) it has full power and authority to enter in and perform this Agreement and that the execution and delivery of this Agreement has been duly authorized; and (b) this Agreement and such Party’s performance hereunder will not breach any other agreement to which the Party is a party or is bound or violate any obligation owed by such Party to any third party.

**5.7 Disclaimer.** EXCEPT FOR THE WARRANTIES SPECIFIED IN THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE LICENSED MATERIALS, SERVICES, BUYER MATERIALS AND BUYER DATA, AND EACH PARTY HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. Licensor does not warrant: (a) that the Licensed Materials will meet Buyer’s requirements; or (b) that the operation of the Product will be uninterrupted or error free.

## **6. Confidentiality.**

**6.1 Confidential Information.** “**Confidential Information**” means any nonpublic information directly or indirectly disclosed by either Party (the “**Disclosing Party**”) to the other Party (the “**Receiving Party**”) or accessible to the Receiving Party pursuant to this Agreement that is designated as confidential or that, given the nature of the information or the circumstances surrounding its disclosure, reasonably should be considered as confidential, including without limitation technical data, trade secrets, know-how, research, inventions, processes, designs, drawings, strategic roadmaps, product plans, product designs and architecture, security information, marketing plans, pricing and cost information, marketing and promotional activities, business plans, customer and supplier information, employee and User information, business and marketing plans, and business processes, and other technical, financial or business information, and any third party information that the Disclosing Party is required to maintain as confidential. Confidential Information will not, however, include any information which: (a) was publicly known or made generally available to the public prior to the time of disclosure; (b) becomes publicly known or made generally available after disclosure through no fault of the Receiving Party; (c) is in the possession of the Receiving Party, without restriction as to use or disclosure, at the time of disclosure by the Disclosing Party; (d) was lawfully received, without restriction as to use or disclosure, from a third party (who does not have an obligation of confidentiality or restriction on use itself); or (e) is developed by the Receiving Party independently from this Agreement and without use of or reference to the Disclosing Party’s Confidential Information or Proprietary Rights. Except for rights expressly granted in this Agreement, each Party reserves all rights in and to its Confidential Information. The Parties agree that the Licensed Materials are Confidential Information of Licensor.

**6.2 Obligations.** The Parties will maintain as confidential and will avoid disclosure and unauthorized use of Confidential Information of the other Party using reasonable precautions. Each Party will protect such Confidential Information with the same degree of care that a prudent person would exercise to protect its own confidential information of a like nature, and to prevent the unauthorized, negligent, or inadvertent use, disclosure, or publication thereof or access thereto. Each Party will restrict Confidential Information to individuals who need to know such Confidential Information and who are bound to confidentiality obligations at least as protective as the restrictions described in this Section 6. Except as necessary for the proper use of the Product, the exercise of a Party’s rights under this Agreement, performance of a Party’s obligations under this Agreement or as otherwise permitted under this Agreement, neither Party will use Confidential Information of the other Party for any purpose except in fulfilling its obligations or exercising its rights under this Agreement. Each Party will promptly notify the other Party if it becomes aware of any unauthorized use or disclosure of the other Party’s Confidential Information, and reasonably cooperate with the other Party in attempts to limit disclosure.

**6.3 Compelled Disclosure.** If and to the extent required by law, including regulatory requirements, discovery request, subpoena, court order or governmental action, the Receiving Party may disclose or produce Confidential Information but will give reasonable prior notice (and where prior notice is not permitted by applicable Law, notice will be given as soon as the Receiving Party is legally permitted) to the Disclosing Party to permit the Disclosing Party to intervene and to request protective orders or confidential treatment therefor or other appropriate remedy regarding such disclosure. Disclosure of any Confidential Information pursuant to any legal requirement will not be deemed to render it non-confidential, and the Receiving Party’s obligations with respect to Confidential Information of the Disclosing Party will not be changed or lessened by virtue of any such disclosure. Notwithstanding any provisions herein, if Buyer is a government agency or entity, Buyer will comply with all Laws applicable to it with respect to disclosure of public information.

**6.4 NDA.** Buyer and Licensor may agree to a separate nondisclosure agreement between Buyer and Licensor (or the respective Affiliates of Buyer and Licensor) (“**NDA**”) that applies to disclosures occurring during the term of the Subscription, in which case the terms and conditions thereof are incorporated herein by reference and will apply instead of subsections 6.1 through 6.3 of this Section 6.

**7. Additional SaaS Service Obligations and Responsibilities.** This Section 7 applies to Subscriptions for Product, or a component of a Product, deployed via SaaS Service only.

**7.1 Acceptable Use; Restrictions on Sensitive Information.**

**7.1.1** Buyer will not intentionally use the Product, component or SaaS Service to: (a) store, download or transmit infringing or illegal content, or any viruses, “Trojan horses” or other harmful code; (b) engage in phishing, spamming, denial-of-service attacks or fraudulent or illegal activity; (c) interfere with or disrupt the integrity or performance of the Product, component or data contained therein or on Licensor’s system or network or circumvent the security features of the Product; or (d) perform penetration testing, vulnerability testing or other security testing on the Product, component or Licensor’s systems or networks or otherwise attempt to gain unauthorized access to the Product or Licensor’s systems or networks.

**7.1.2** Buyer will not use the SaaS Services to store or process Highly Sensitive Information unless Licensor specifically purchases a SaaS Service Subscription designed to be used with Highly Sensitive Information. “**Highly Sensitive Information**” means, for purposes of this Agreement: (1) special categories of data enumerated in applicable Data Protection Laws, including European Union Regulation 2016/679, Article 9(1) or any successor legislation; (2) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act (as amended and supplemented) (“**HIPAA**”); (3) credit, debit, or other payment card data, including bank account numbers; (4) social security numbers, driver’s license numbers, or other government identification numbers; (5) other information subject to additional protections or regulation under specific laws such as the Children’s Online Privacy Protection Act or Gramm-Leach-Bliley Act (or related rules or regulations). Supplier shall have no responsibility for Highly Sensitive Information where the SaaS Service is not approved by Licensor to be used with Highly Sensitive Information.

**7.1.3** Licensor may suspend Buyer’s or a User’s right to access or use any portion or all of the SaaS Service immediately upon notice to Buyer (a) if Licensor, after reasonable due diligence given the nature and severity of the issue, reasonably determines that: (i) Buyer or a User’s use of the SaaS Service poses a material risk to the security or operation of Licensor’s systems, the SaaS Service or the systems or data of any other customer, or (ii) Buyer or a User’s use of the SaaS Service violates this Section 7.1 or is illegal or fraudulent; or (b) Buyer fails to pay any undisputed amounts within 30 days after notice of past due amounts. To the extent reasonably practicable, Licensor will limit the suspension of the SaaS Service pursuant to subsection (a) as needed to mitigate the applicable risk. Licensor will promptly restore the SaaS Service to Buyer upon resolution of the issue and/or payment of the outstanding amounts (as applicable).

**7.2 Buyer Data and Buyer Materials.**

**7.2.1** Buyer is and will continue to be the sole and exclusive owner of all Buyer Materials, Buyer Data and other Confidential Information of Buyer, including all Proprietary Rights therein. Nothing in this Agreement will be construed or interpreted as granting to Licensor any rights of ownership or any other proprietary rights in or to the Buyer Data and Buyer Materials.

**7.2.2** Buyer will obtain all necessary consents, authorizations and rights and provide all necessary notices and disclosures in order to provide Buyer Data to Licensor and for Licensor to use Buyer Data in the performance of its obligations in accordance with the terms and condition of this Agreement, including any access or transmission to third parties with whom Buyer shares or permits access to Buyer Data.

**7.2.3** The Parties agree that Buyer Data and Buyer Materials are Confidential Information of Buyer. Buyer hereby grants to Licensor a nonexclusive, nontransferable (except in connection with an assignment permitted under Section 12.2), revocable license, under all Proprietary Rights, to reproduce and use Buyer Materials and Buyer Data solely for the purpose of, and to the extent necessary for, performing Licensor’s obligations under this Agreement. In no event will Licensor access, use or disclose to any third party any Buyer Data or any Buyer Materials for any purpose whatsoever other than as necessary for the purpose of providing the Product and Services to Buyer and performing its obligations under this Agreement. Licensor will not aggregate, anonymize or create any data derivatives of Buyer Data other than as necessary to provide the Product or Services and to perform its obligations in accordance with the terms and conditions of this Agreement.

**7.2.4** Buyer will have full access to, and has the right to review and retain, the entirety of Buyer Data contained in the Product. At no time will any computer or electronic records containing Buyer Data be stored or held in a form or manner not readily accessible to Buyer through the ordinary operation of the Product. Licensor will provide to Buyer all passwords, codes, comments, keys and documentation necessary for such access and use of the Product, and Buyer will be entitled to delete, or have Licensor delete, Buyer Data as expressly specified by Buyer.

**7.3 System Data.** To the extent that System Data identifies or permits, alone or in conjunction with other data, identification, association, or correlation of or with Buyer, its Affiliates, Users, customers, suppliers or other persons interacting with any of the foregoing, or any Confidential Information of Buyer or any device as originating through or interacting with Buyer or its Affiliates (“**Identifiable System Data**”), Licensor may only collect and use Identifiable System Data internally to administer, provide and improve the Product and Services as a generally available service offering, to identify opportunities for Buyer to optimize its use of the Product, including the provision of additional training, and to identify to Buyer complementary uses of Licensor’s other products and services. Licensor will not target any data analysis at, or otherwise use any Identifiable System Data to derive or attempt to derive information regarding, Buyer and its Affiliates, their businesses, operations, finances, users, customers, prospective customers, suppliers or other persons interacting with Buyer and its Affiliates. Licensor will not target any development efforts arising from its use of Identifiable System Data at any person on the basis of the intended recipient’s relationship with Buyer or any of its Affiliates or the intended recipient being in same industry or market as Buyer or any of its Affiliates. Licensor will not use or disclose any Identifiable System Data for any other purpose unless otherwise agreed in writing by the Parties, and will, except for the use permitted in this Section, maintain the confidentiality and security of Identifiable System Data as Confidential Information.

**7.4 Use of Other Data.** Notwithstanding the foregoing, nothing in this Agreement will restrict: (a) Licensor's use of System Data or data derived from System Data that does not identify or permit, alone or in conjunction with other data, identification, association, or correlation of or with (i) Buyer, its Affiliates, Users, customers, suppliers or other persons interacting with Buyer and its Affiliates or any Confidential Information of Buyer, or (ii) any device (e.g. computer, mobile telephone, or browser) used to access or use the Product as originating through Buyer or its Affiliates or interacting with Buyer or its Affiliates; or (b) either Party's use of any data, records, files, content or other information related to any third party that is collected, received, stored or maintained by a Party independently from this Agreement.

**7.5 Security; Breach Notification.** Licensor will comply with the security practices (if any) incorporated or referenced in the Product Listing and Documentation for the Product, provided however that at all times Licensor will, consistent with industry standard practices, implement and maintain physical, administrative and technical safeguards and other security measures: (a) to maintain the security and confidentiality of Buyer Data; and (b) to maintain the availability and integrity of Buyer Data and to protect Buyer Data from known or reasonably anticipated threats or hazards to its security, including accidental loss, unauthorized use, access, alteration or disclosure. Licensor will inform Buyer promptly upon discovery of any material unauthorized access to, any unauthorized loss, use or disclosure of any Buyer Data ( a "**Security Incident**"), provided that such notification is not prohibited by Law. Licensor will investigate the cause of the Security Incident and take reasonable steps to prevent further unauthorized access, loss, use or disclosure of Buyer Data. At Buyer's request and cost, Licensor will reasonably cooperate with Buyer in complying with its obligations under applicable law pertaining to responding to a Security Incident. Licensor's obligation to report or respond to a Security Incident under this Section is not an acknowledgement by Licensor of any fault or liability with respect to the Security Incident.

**7.6 Data Protection Legislation.**

**7.6.1** Each Party will comply with all Data Protection Laws, and any implementations of such Laws, applicable to its performance under this Agreement. The Parties acknowledge and agree that they will consider in good faith implementing any codes of practice and best practice guidance issued by relevant authorities as they apply to applicable country specific Data Protection Laws or their implementations.

**7.6.2** Without limiting the generality of the foregoing, if Licensor is collecting or furnishing Personal Data to Buyer or if Licensor is processing, storing or transferring Personal Data on behalf of Buyer, then Licensor and Buyer and/or their Affiliate(s), as applicable, will agree to supplemental privacy and security terms consistent with applicable Law. Unless Licensor and Buyer expressly agree to be bound by other terms and conditions that reflect their respective legal obligations with respect to Personal Data, Licensor and Buyer agree to the terms and conditions of the attached Data Processing Addendum. For the avoidance of doubt, no Personal Data should be processed or transferred under this Agreement without Privacy and Security Terms necessary for compliance with applicable Law.

**7.7 Remedies.** Each Party agrees that in the event of a breach or threatened breach of this Section 7, the non-breaching Party will be entitled to injunctive relief against the breaching Party in addition to any other remedies to which the non-breaching Party may be entitled.

**8. Limitations of Liability.**

**8.1 Disclaimer; General Cap.** SUBJECT TO SECTIONS 8.2, 8.3 AND 8.4, IN NO EVENT WILL (a) EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND (b) EITHER PARTY'S AGGREGATE LIABILITY UNDER THIS AGREEMENT, WHETHER SUCH DAMAGES ARE BASED IN CONTRACT, TORT OR OTHER LEGAL THEORY, EXCEED THE FEES AND OTHER AMOUNTS PAID AND REQUIRED TO BE PAID UNDER THIS AGREEMENT IN THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO THE DAMAGES.

**8.2 Exception for Gross Negligence, Willful Misconduct or Fraud.** THE EXCLUSIONS OF AND LIMITATIONS ON LIABILITY SET FORTH IN SECTION 8.1(a) AND (b) WILL NOT APPLY TO A PARTY'S GROSS NEGLIGENCE, WILLFUL MISCONDUCT, OR FRAUD.

**8.3 Exception for Certain Indemnification Obligations.** THE EXCLUSIONS OF AND LIMITATIONS ON LIABILITY SET FORTH IN SECTIONS 8.1(a) AND (b) WILL NOT APPLY TO ANY COSTS OF DEFENSE AND ANY AMOUNTS AWARDED AGAINST THE INDEMNIFIED PARTY BY A COURT OF COMPETENT JURISDICTION OR AGREED UPON PURSUANT TO SETTLEMENT AGREEMENT THAT ARE SUBJECT TO SUCH PARTY'S INDEMNIFICATION AND DEFENSE OBLIGATIONS UNDER THIS AGREEMENT.

**8.4 Special Cap for Security Breach.**

**8.4.1** FOR SAAS SERVICE SUBSCRIPTIONS, THE EXCLUSIONS OF AND LIMITATIONS ON LIABILITY SET FORTH IN SECTIONS 8.1(a) AND (b) WILL NOT APPLY TO, AND INSTEAD SECTION 8.4.2 WILL APPLY TO: (a) GOVERNMENT FINES AND PENALTIES INCURRED BY BUYER AND BUYER'S OUT-OF-POCKET, REASONABLE AND DOCUMENTED COSTS OF INVESTIGATION, NOTIFICATION, REMEDIATION AND MITIGATION SPECIFIED IN SECTION 9.5 RESULTING FROM ANY SECURITY INCIDENT RESULTING FROM BREACH OF LICENSOR'S OBLIGATIONS UNDER THE PRIVACY AND SECURITY TERMS OR ANY VIOLATION BY LICENSOR OF DATA PROTECTION LAWS, AND LICENSOR'S OBLIGATIONS WITH RESPECT THERETO PURSUANT TO SECTION 9.5; AND (b) ANY LIABILITIES ARISING FROM CLAIMS BROUGHT BY THIRD PARTIES AGAINST BUYER ARISING FROM ANY SECURITY INCIDENT RESULTING FROM BREACH OF LICENSOR'S OBLIGATIONS UNDER ANY PRIVACY AND SECURITY TERMS OR ANY VIOLATION BY LICENSOR OF DATA PROTECTION LAWS, INCLUDING OUT-OF-POCKET COSTS OF DEFENSE AND ANY AMOUNTS AWARDED AGAINST BUYER BY A COURT OF COMPETENT JURISDICTION OR AGREED UPON PURSUANT TO A SETTLEMENT AGREEMENT.

**8.4.2** FOR SAAS SERVICE SUBSCRIPTIONS, LICENSOR'S AGGREGATE LIABILITY UNDER THIS AGREEMENT FOR ANY SECURITY INCIDENT RESULTING FROM BREACH OF LICENSOR'S OBLIGATIONS UNDER ANY PRIVACY AND SECURITY TERMS OR RESULTING FROM BREACH OF LICENSOR'S OBLIGATIONS UNDER

THE PRIVACY AND SECURITY TERMS OR ANY VIOLATION BY LICENSOR OF DATA PROTECTION LAWS, INCLUDING GOVERNMENT FINES AND PENALTIES INCURRED BY BUYER AND BUYER'S OUT-OF-POCKET, REASONABLE AND DOCUMENTED COSTS SET FORTH IN SECTION 9.5 AND LICENSOR'S INDEMNIFICATION AND DEFENSE OBLIGATIONS PURSUANT TO SECTION 9.1(b) AND ITS OBLIGATIONS PURSUANT TO SECTION 9.5 AND LICENSOR'S OBLIGATIONS WITH RESPECT THERETO PURSUANT TO SECTION 9.5, WHETHER SUCH DAMAGES ARE BASED IN CONTRACT, TORT OR OTHER LEGAL THEORY, WILL NOT EXCEED (IN LIEU OF AND NOT IN ADDITION TO THE AMOUNT SET FORTH IN SECTION 8.1) THREE TIMES THE FEES AND OTHER AMOUNTS PAID AND REQUIRED TO BE PAID UNDER THIS AGREEMENT IN THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO THE DAMAGES.

#### **9. Indemnification.**

**9.1 Licensor Indemnity.** Licensor will, at its expense, defend Buyer and its Affiliates and their respective officers, directors, employees, agents and representatives (collectively "**Buyer Indemnified Parties**") from and against any and all claims, actions, proceedings and suits brought by a third party (including government investigations), ("**Claims**") to the extent arising out of or alleging of any of the following: (a) infringement, misappropriation or violation of any Proprietary Rights by the Licensed Materials or Buyer's use thereof as permitted under this Agreement; and (b) any unauthorized access, use or disclosure of Buyer Data resulting from breach of Licensor's obligations under the Privacy and Security Terms or any violation by Licensor of Data Protection Laws. Licensor will pay all costs, damages and amounts finally awarded by a court or agreed upon in settlement (as set forth in Section 9.3 below) and any government fines and penalties assessed against or incurred by Buyer in any such Claims.

**9.2 Buyer Indemnity.** Buyer will, at its expense, defend Licensor and its Affiliates and their respective officers, directors, employees, agents and representatives (collectively "**Licensor Indemnified Parties**") from and against any and all Claims to the extent arising out of or alleging of any of the following: (a) infringement, misappropriation or violation of any Proprietary Rights by the Buyer Materials or Buyer Data or Licensor's use thereof as permitted under this Agreement; and (b) any unauthorized or unlawful receipt, processing, transmission or storage of Buyer Data by Licensor in the performance of its obligations as permitted under this Agreement resulting from breach of Buyer's obligations under Section 7.2.2. Buyer will pay all costs, damages and amounts finally awarded by a court or agreed upon in settlement (as set forth in Section 9.3 below) and any government fines and penalties assessed against or incurred by Licensor in any such Claims. Notwithstanding any provisions herein, if Buyer is a government entity, this Section 9.2 will not apply except as permitted by applicable Law.

**9.3 Process.** The party(ies) seeking indemnification pursuant to this Section 9 (each, an "**Indemnified Party**" and collectively, the "**Indemnified Parties**") will give the other Party (the "**Indemnifying Party**") prompt notice of each Claim for which it seeks indemnification, provided that failure or delay in providing such notice will not release the Indemnifying Party from any obligations hereunder except to the extent that the Indemnifying Party is prejudiced by such failure. The Indemnified Parties will give the Indemnifying Party their reasonable cooperation in the defense of each Claim for which indemnity is sought, at the Indemnifying Party's expense. The Indemnifying Party will keep the Indemnified Parties informed of the status of each Claim. An Indemnified Party may participate in the defense at its own expense. The Indemnifying Party will control the defense or settlement of the Claim, provided that the Indemnifying Party, without the Indemnified Parties' prior written consent: (a) will not enter into any settlement that; (i) includes any admission of guilt or wrongdoing by any Indemnified Party; (ii) imposes any financial obligations on any Indemnified Party that Indemnified Party is not obligated to pay under this Section 9; (iii) imposes any non-monetary obligations on any Indemnified Party; and (iv) does not include a full and unconditional release of any Indemnified Parties; and (b) will not consent to the entry of judgment, except for a dismissal with prejudice of any Claim settled as described in (a). The Indemnifying Party will ensure that any settlement into which it enters for any Claim is made confidential, except where not permitted by applicable Law.

**9.4 Infringement Remedy.** In addition to Licensor's obligations under Section 9.1, if the Product or other Licensed Materials is held, or in Licensor's opinion is likely to be held, to infringe, misappropriate or violate any Proprietary Rights, or, if based on any claimed infringement, misappropriation or violation of Proprietary Rights, an injunction is obtained, or in Licensor's opinion an injunction is likely to be obtained, that would prohibit or interfere with Buyer's use of the Licensed Materials under this Agreement, then Licensor will at its option and expense either: (a) procure for Buyer the right to continue using the affected Licensed Materials in accordance with the license granted under this Agreement; or (b) modify or replace the affected Licensed Materials so that the modified or replacement Licensed Materials are reasonably comparable in functionality, interoperability with other software and systems, and levels of security and performance and do not infringe, misappropriate or violate any third-party Proprietary Rights. If, in such circumstances, Licensor cannot not successfully accomplish any of the foregoing actions on a commercially reasonable basis, Licensor will notify Buyer and either Party may terminate the Subscription and this Agreement, in which case Licensor will refund to Buyer any fees prepaid to Licensor by Buyer prorated for the unused portion of the Subscription. For clarity, Licensor's indemnification and defense obligations under this Section include infringement Claims based on use of the Licensed Materials by Buyer Indemnified Parties following an initial infringement Claim except that, if Licensor responds to an infringement Claim by accomplishing the solution in (b), Licensor will have no obligation to defend and indemnify Buyer for infringement Claims arising from Buyer's use after the accomplishment of (b) of the infringing Licensed Materials for which Licensor provided modified or replacement Licensed Materials and a reasonable time to implement the modified or replacement Licensed Materials.

**9.5 Security Breach Remedy.** In the case of a SaaS Service Subscription, in addition to Licensor's obligations under Section 9.1, in the event of any Security Incident resulting from breach of Licensor's obligations under any Privacy and Security Terms or any violation by Licensor of Data Protection Laws, Licensor will pay the government fines and penalties and other out-of-pocket costs incurred by Buyer, to the extent reasonable and documented, for (a) investigating and responding to the Security Incident; (b) legal advice regarding the Security Incident; (c) providing notification to affected individuals, applicable government and relevant industry self-regulatory agencies and the media; (d) providing credit monitoring and/or identity theft services to affected individuals; (e) operating a call center to respond to questions from

affected individuals; and (f) any other investigation, mitigation, remediation, or notification required by law or regulators to be undertaken by Buyer in response to such Security Incident.

#### **9.6 Limitations.**

**9.6.1** Licensor will have no liability or obligation under this Section 9 with respect to any infringement Claim to the extent attributable to any: (a) modifications to the Licensed Materials not provided by Licensor or its Personnel; (b) use of the Product in combination with third-party equipment or software not provided or made accessible by Licensor or not specifically referenced for use with the Licensed Materials by the Product Listing or Documentation; or (c) use of the Licensed Materials by Buyer in breach of this Agreement. Licensor's liability under this Section 9 with respect to any infringement Claim that is attributable to use of the Product in combination with third-party equipment or software provided or made accessible by Licensor or specifically referenced by the Product Listing or Documentation is limited to Licensor's proportional share of defense costs and indemnity liability based on the lesser of: (i) the value of the contribution of the Licensed Materials to the total value of the actual or allegedly infringing combination; or (ii) the relative contribution of the Licensed Materials to the actual or allegedly infringed claims (e.g., the Licensed Materials are alleged to satisfy one limitation of a claim with four separate limitations and Licensor would be responsible for a 25% share of the defense and indemnity obligations).

**9.6.2 Buyer will have no liability or obligation under this Section 9** with respect to any infringement Claim to the extent attributable to any: (a) modifications to the Buyer Materials or Buyer Data not provided by Buyer or its Personnel; or (b) use of the Buyer Materials or Buyer Data by Licensor in breach of this Agreement.

**9.6.3 This Section 9** states the entire liability of Licensor with respect to infringement, misappropriation or violation of Proprietary Rights of third parties by any Licensed Materials or any part thereof or by any use thereof by Buyer, and this Section 9 states the entire liability of Buyer with respect to infringement, misappropriation or violation of Proprietary Rights of third parties by any Buyer Materials, Buyer Data or any part thereof or by any use, receipt, storage or processing thereof by Licensor.

**9.7 Not Limiting.** The foregoing indemnities will not be limited in any manner whatsoever by any required or other insurance coverage maintained by a Party.

#### **10. Term and Termination.**

**10.1 Term.** This Agreement will continue in full force and effect until conclusion of the Subscription, unless terminated earlier by either Party as provided by this Agreement.

**10.2 Termination.** Either Party may terminate the Subscription or this Agreement if the other Party materially breaches this Agreement and does not cure the breach within 30 days following its receipt of written notice of the breach from the non-breaching Party. In the case of a SaaS Service Subscription, termination by Licensor pursuant to this Section does not prejudice Buyer's right, and Licensor's obligation, to extract or assist with the retrieval or deletion of Buyer Data as set forth in Section 10.3.2 following such termination.

#### **10.3 Effect of Termination.**

**10.3.1** Upon termination or expiration of the Subscription or this Agreement, Buyer's right to use the Product licensed under such Subscription will terminate, and Buyer's access to the Product and Service provided under such Subscription may be disabled and discontinued. Termination or expiration of any Subscription purchased by Buyer from Licensor will not terminate or modify any other Subscription purchased by Buyer from Licensor.

**10.3.2** Within 45 days (or such other period as may be agreed upon by the Parties) following termination or expiration of any SaaS Service Subscription for any reason and on Buyer's written request at any time before termination or expiration, Licensor will extract from the Product and/or Licensor's Computing Environment (as applicable) and return to Buyer all Buyer Data, or if Buyer is able directly to retrieve or delete Buyer Data using the SaaS Service, then for a period of 45 days (or such other period as may be agreed upon by the Parties) following termination or expiration of this Agreement for any reason, Buyer may retrieve or delete Buyer Data itself with support from Licensor as reasonably requested by Buyer. If Buyer retrieves or deletes Buyer Data itself, Licensor will assist Buyer, as reasonably requested by Buyer, in validating whether the retrieval or deletion was successful. Buyer Data must be provided or extractable in a then-current, standard nonproprietary format. Notwithstanding anything herein to the contrary, Licensor's duty to return or enable Buyer's retrieval or deletion of the Buyer Data pursuant to this Section 10.3.2 may be delayed but will not be discharged due to the occurrence of any Force Majeure event. Following delivery to Buyer of the Buyer Data and Buyer's confirmation thereof, or Buyer's retrieval or deletion of Buyer Data and Licensor's validation thereof or expiration of the applicable period, whichever is soonest, Licensor may, and within a reasonable time thereafter will, permanently delete and remove Buyer Data (if any) from its electronic and hard copy records and will, upon Buyer's request, certify to such deletion and removal to Buyer in writing. If Licensor is not able to delete any portion of the Buyer Data or Buyer Confidential Information, it will remain subject to the confidentiality, privacy and data security terms of this Agreement.

**10.3.3 Sections 4** (Proprietary Rights), 6 (Confidentiality), 7.2.1 (Buyer Data and Buyer Materials), 8 (Limitations of Liability), 9 (Indemnification), 10.3 (Effect of Termination), 11 (Insurance), 12(General) and 13 (Definitions) and any perpetual license granted under this Agreement, together with all other provisions of this Agreement that may reasonably be interpreted or construed as surviving expiration or termination, will survive the expiration or termination of this Agreement for any reason; but the nonuse and nondisclosure obligations of Section 6 will expire five years following the expiration or termination of this Agreement, except with respect to, and for as long as, any Confidential Information constitutes a trade secret.

#### **11. Insurance.**

**11.1 Coverages.** Each Party will obtain and maintain appropriate insurance necessary for implementing and performing under this Agreement in accordance with applicable Law and in accordance with the requirements of this Section 11. Subject to Licensor's right to self-insure as described below, Licensor will at its own cost and expense, acquire and continuously maintain the following insurance coverage during the term of this Agreement and for one year after:

**11.1.1** Commercial General Liability insurance, including all major coverage categories, including premises-operations, property damage, products/completed operations, contractual liability, personal and advertising injury with limits of \$1,000,000 per occurrence and \$2,000,000 general aggregate, and \$5,000,000 products/completed operations aggregate;

**11.1.2** Professional Liability insurance, covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering Services in connection with this Agreement including acts, errors or omissions in rendering computer or information technology Services, proprietary rights infringement, data damage/destruction/corruption, failure to protect privacy, unauthorized access, unauthorized use, virus transmission and denial of service from network security failures with a minimum limit of \$2,000,000 each claim and annual aggregate;

**11.1.3** If a SaaS Service Subscription, Cyber Liability or Technology Errors and Omissions, with limits of \$2,000,000 each claim and annual aggregate, providing for protection against liability for: (a) system attacks; (b) denial or loss of service attacks; (c) spread of malicious software code; (d) unauthorized access and use of computer systems; (e) liability arising from loss or disclosure of personal or corporate confidential data; (f) cyber extortion; (g) breach response and management coverage; (h) business interruption; and (i) invasion of privacy; and

**11.1.4** If a SaaS Service Subscription, Computer Crime Insurance with limits of \$1,000,000 and Employee Theft/Buyer Insurance Coverage with limits of \$500,000.

**11.2 Umbrella Insurance; Self-Insurance.** The limits of insurance may be satisfied by any combination of primary and umbrella/excess insurance. In addition, either Party may satisfy its insurance obligations specified in this Agreement through a self-insured retention program. Upon request by Buyer, Licensor will provide evidence of Licensor's self-insurance program in a formal declaration (on Licensor's letterhead, if available) that declares Licensor is self-insured for the type and amount of coverage as described in Section 11.1. Licensor's declaration may be in the form of a corporate resolution or a certified statement from a corporate officer or an authorized principal of Licensor. The declaration also must identify which required coverages are self-insured and which are commercially insured.

**11.3 Certificates and Other Requirements.** Prior to execution of this Agreement and annually thereafter during the term, Buyer may request that Licensor furnish to Buyer a certificate of insurance evidencing the coverages set forth above. Licensor's Commercial General Liability and any umbrella insurance relied upon to meet the obligations in this Section will be primary and non-contributory coverage and the policies will not contain any intra-insured exclusions as between insured persons or organizations. Licensor's Commercial General Liability policy will provide a waiver of subrogation in favor of Buyer and its Affiliates. The stipulated limits of coverage above will not be construed as a limitation of any potential liability to Buyer, and failure to request evidence of this insurance will not be construed as a waiver of Licensor's obligation to provide the insurance coverage specified.

## **12. General.**

**12.1 Applicable Law.** This Agreement will be governed and interpreted under the laws of the State of New York, excluding its principles of conflict of laws. The Parties agree that any legal action or proceeding relating to this Agreement will be instituted solely in the state and federal courts located in New York City, New York. Each Party irrevocably submits to the jurisdiction of such courts, and each Party waives any objection that it may have to the laying of the venue of any such action or proceeding in the manner provided in this Section. The Parties agree that the United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement.

**12.2 Assignment.** Neither Party may assign or transfer this Agreement or any rights or delegate any duties herein without the prior written consent of the other Party, which will not be reasonably withheld, delayed or conditioned. Notwithstanding the foregoing, and without gaining the other Party's written consent, Licensor may assign this Agreement, in its entirety, and delegate its obligations to its Affiliates or to any entity acquiring all or substantially all of its assets, whether by sale of assets, sale of stock, merger or otherwise and Buyer may assign this Agreement, in its entirety, to any Affiliates or entity acquiring all or substantially all of its assets related to Buyer's account or the Buyer's entire business, whether by sale of assets, sale of stock, merger or otherwise. Any attempted assignment, transfer or delegation in contravention of this Section will be null and void. This Agreement will inure to the benefit of the Parties hereto and their permitted successors and assigns.

**12.3 Entire Agreement.** This Agreement constitutes the entire agreement between the Parties relating to the subject matter hereof, and there are no other representations, understandings or agreements between the Parties relating to the subject matter hereof. This Agreement is solely between Buyer and Licensor. Neither Amazon Web Services, Inc. nor any of its Affiliates are a party to this Agreement and none of them will have any liability or obligations hereunder. The terms and conditions of this Agreement will not be changed, amended, modified or waived unless such change, amendment, modification or waiver is in writing and signed by authorized representatives of the Parties. NEITHER PARTY WILL BE BOUND BY, AND EACH SPECIFICALLY OBJECTS TO, ANY PROVISION THAT IS DIFFERENT FROM OR IN ADDITION TO THIS AGREEMENT (WHETHER PROFFERED ORALLY OR IN ANY QUOTATION, PURCHASE ORDER, INVOICE, SHIPPING DOCUMENT, ONLINE TERMS AND CONDITIONS, ACCEPTANCE, CONFIRMATION, CORRESPONDENCE, OR OTHERWISE), UNLESS SUCH PROVISION IS SPECIFICALLY AGREED TO IN A WRITING SIGNED BY BOTH PARTIES.

**12.4 Export Laws.** Each Party will comply with all applicable customs and export control laws and regulations of the United States and/or such other country, in the case of Buyer, where Buyer or its Users use the Product or Services, and in the case of Licensor, where Licensor provides the Product or Services. Each Party certifies that it and its Personnel are not on any of the relevant U.S. Government Lists of prohibited persons, including but not limited to the Treasury Department's List of Specially Designated Nationals and the Commerce Department's list of Denied Persons. Neither Party will export, re-export, ship, or otherwise transfer the Licensed Materials, Services or Buyer Data to any country subject to an embargo or other sanction by the United States or other applicable jurisdiction.

**12.5 Force Majeure.** Neither Party will be liable hereunder for any failure or delay in the performance of its obligations in whole or in part, on account of riots, fire, flood, earthquake, explosion, epidemics, war, strike or labor disputes (not involving the Party claiming force majeure), embargo, civil or military authority, act of God, governmental action or other

causes beyond its reasonable control and without the fault or negligence of such Party or its Personnel and such failure or delay could not have been prevented or circumvented by the non-performing Party through the use of alternate sourcing, workaround plans or other reasonable precautions (a “**Force Majeure Event**”). If a Force Majeure Event continues for more than 14 days for any Subscription with Entitlement Pricing, Buyer may cancel the unperformed portion of the Subscription and receive a pro rata refund of any fees prepaid by Buyer to Licensor for such unperformed portion.

**12.6 Government Rights.** As defined in FARS §2.101, the Product and Documentation are “commercial items” and according to DFARS §252.227 and 7014(a)(1) and (5) are deemed to be “commercial computer software” and “commercial computer software documentation”. Consistent with FARS §12.212 and DFARS §227.7202, any use, modification, reproduction, release, performance, display or disclosure of such commercial software or commercial software documentation by the U.S. government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

**12.7 Headings.** The headings throughout this Agreement are for reference purposes only, and the words contained therein will in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

**12.8 No Third-Party Beneficiaries.** Except as specified in Section 9 with respect to Buyer Indemnified Parties and Licensor Indemnified Parties, nothing express or implied in this Agreement is intended to confer, nor will anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations or liabilities whatsoever.

**12.9 Notices.** To be effective, notice under this Agreement must be given in writing. Each Party consents to receiving electronic communications and notifications from the other Party in connection with this Agreement. Each Party agrees that it may receive notices from the other Party regarding this Agreement: (a) by email to the email address designated by such Party as a notice address for the Standard Contract; (b) by personal delivery; (c) by registered or certified mail, return receipt requested; or (d) by nationally recognized courier service. Notice will be deemed given upon written verification of receipt.

**12.10 Nonwaiver.** Any failure or delay by either Party to exercise or partially exercise any right, power or privilege under this Agreement will not be deemed a waiver of any such right, power or privilege under this Agreement. No waiver by either Party of a breach of any term, provision or condition of this Agreement by the other Party will constitute a waiver of any succeeding breach of the same or any other provision hereof. No such waiver will be valid unless executed in writing by the Party making the waiver.

**12.11 Publicity.** Neither Party will issue any publicity materials or press releases that refer to the other Party or its Affiliates, or use any trade name, trademark, service mark or logo of the other Party or its Affiliates in any advertising, promotions or otherwise, without the other Party’s prior written consent.

**12.12 Relationship of Parties.** The relationship of the Parties will be that of independent contractors, and nothing contained in this Agreement will create or imply an agency relationship between Buyer and Licensor, nor will this Agreement be deemed to constitute a joint venture or partnership or the relationship of employer and employee between Buyer and Licensor. Each Party assumes sole and full responsibility for its acts and the acts of its Personnel. Neither Party will have the authority to make commitments or enter into contracts on behalf of, bind, or otherwise oblige the other Party.

**12.13 Severability.** If any term or condition of this Agreement is to any extent held invalid or unenforceable by a court of competent jurisdiction, the remainder of this Agreement will not be affected thereby, and each term and condition will be valid and enforceable to the fullest extent permitted by law.

**12.14 Subcontracting.** Licensor may use Subcontractors in its performance under this Agreement, provided that: (a) Licensor remains responsible for all its duties and obligations hereunder and the use of any Subcontractor will not relieve or reduce any liability of Licensor or cause any loss of warranty under this Agreement; and (b) Licensor agrees to be directly liable for any act or omission by such Subcontractor to the same degree as if the act or omission were performed by Licensor such that a breach by a Subcontractor of the provisions of this Agreement will be deemed to be a breach by Licensor. The performance of any act or omission under this Agreement by a Subcontractor for, by or through Licensor will be deemed the act or omission of Licensor. Upon request, Licensor will identify to Buyer any Subcontractors performing under this Agreement, including any that have access to Buyer Data, and such other information reasonably requested by Buyer about such subcontracting.

### **13. Definitions.**

**13.1 “Affiliate”** means, with respect to a Party, any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with such Party.

**13.2 “AWS Marketplace”** means the marketplace operated by Amazon Web Services, Inc. located at <https://aws.amazon.com/marketplace/> as it may be updated from time to time.

**13.3 “Buyer Data”** means all data, records, files, information or content, including text, sound, video, images and software, that is (a) input or uploaded by Buyer or its Users to or collected, received, transmitted, processed, or stored by Buyer or its Users using the Product or SaaS Service in connection with this Agreement, or (b) derived from (a). Buyer Data is Confidential Information of Buyer.

**13.4 “Buyer Materials”** means any property, items or materials, including Buyer Data, furnished by Buyer to Licensor for Licensor’s use in the performance of its obligations under this Agreement.

**13.5 “Buyer’s Computing Environment”** means the Buyer computing environment in which Licensor authorizes use of the Subscription.

**13.6 “Contractor”** means any third party contractor of Buyer or other third party performing services for Buyer, including outsourcing suppliers.

**13.7 “Data Protection Law”** means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including Regulation 2016/679 (General Data Protection Regulation) (“GDPR”), and Cal. Civ. Code 1798.100 et seq. (California Consumer Privacy Act) (“CCPA”).

**13.8 “Documentation”** means the user guides, manuals, instructions, specifications, notes, documentation, printed updates, “read-me” files, release notes and other materials related to the Product (including all information included or incorporated by reference in the applicable Product Listing), its use, operation or maintenance, together with all enhancements, modifications, derivative works, and amendments to those documents, that Licensor publishes or provides under this Agreement.

**13.9 “Entitlement Pricing”** means any Subscription pricing model where Buyer purchases a quantity of usage upfront, include prepaid and installment payment pricing models.

**13.10 “International Data Transfer Mechanism”** means the special protections that some jurisdictions require two or more parties that transfer information across international borders to adopt to make the transfer lawful, e.g., Standard Contractual Clauses, Binding Corporate Rules, or statutory obligations that require the parties to adopt certain technical, organizational, or contractual measures. “Transfer,” in the context of an International Data Transfer Mechanism, means to disclose or move personal data from a storage location in one jurisdiction to another, or to permit a party in one jurisdiction to access Personal Data that the other party stores in another jurisdiction that requires an International Data Transfer Mechanism.

**13.11 “Licensed Materials”** means the Product, Documentation and any other items, materials or deliverables that Licensor provides, or is obligated to provide, as part of a Subscription.

**13.12 “Licensor’s Computing Environment”** means the computing infrastructure and systems used by Licensor to provide the Product via SaaS Service.

**13.13 “Open Source Software”** means software distributed under a licensing or distribution model that is publicly available and makes the source code to such software available to licensees for use, modification and redistribution.

**13.14 “Personal Data”** means information the Buyer Data that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a data subject. “Personal Data” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “Personal Information,” as context requires, to the extent such information forms part of the Buyer Data.

**13.15 “Personnel”** means a Party or its Affiliate’s directors, officers, employees, non-employee workers, agents, auditors, consultants, contractors, subcontractors and any other person performing services on behalf of such Party (but excludes the other Party and any of the foregoing of the other Party).

**13.16 “Privacy and Security Terms”** means Section 7.5, the attached Data Protection Addendum (if applicable), and any other terms and conditions regarding the privacy and security of data agreed upon by the parties that are a part of this Agreement, whether in an addendum or amendment to this Standard Contract.

**13.17 “Product Listing”** means the description of Product and other product information listed on the AWS Marketplace and offered by Licensor or its authorized reseller, including Support Services and Licensor’s policies and procedures incorporated or referenced in the product information. The Product Listing may also describe, incorporate or reference Licensor’s security practices or disclosures concerning Open Source Software.

**13.18 “Product”** means the computer software and any associated data, content and/or services identified in the applicable Product Listing that Licensor provides or is obligated to provide as part of a Subscription, including any patches, bug fixes, corrections, remediation of security vulnerabilities, updates, upgrades, modifications, enhancements, derivative works, new releases and new versions of the foregoing that Licensor provides, or is obligated to provide, as part of the Subscription.

**13.19 “Proprietary Rights”** means all intellectual property and proprietary rights throughout the world, whether now known or hereinafter discovered or invented, including, without limitation, all: (a) patents and patent applications; (b) copyrights and mask work rights; (c) trade secrets; (d) trademarks; (e) rights in data and databases; and (f) analogous rights throughout the world.

**13.20 “SaaS Service”** means access and use of the Product, or a component of a Product, as deployed and hosted by Licensor in the Licensor’s Computing Environment, and any software and other technology provided or made accessible by Licensor in connection therewith (and not as a separate product or service) that Buyer is required or has the option to use in order to access and use the Product.

**13.21 “Services”** means all services and tasks that Licensor provides or is obligated to provide under this Agreement, including without limitation Support Services.

**13.22 “Subcontractor”** means any third party subcontractor or other third party to whom Licensor delegates any of its duties and obligations under this Agreement.

**13.23 “Subscription”** means a Product subscription for a specific use capacity purchased by Buyer and fulfilled by Licensor for the licensing and provision of Product, whether deployed in Buyer’s Computing Environment and/or provided as a SaaS Service through Licensor’s Computing Environment.

**13.24 “Support Services”** means the support and maintenance services for the Product that Licensor provides, or is obligated to provide, as described in the Product Listing.

**13.25 “System Data”** means data and data elements (other than Buyer Data) collected by the Product, SaaS Service or Licensor’s Computer Environment regarding configuration, environment, usage, performance, vulnerabilities and security of the Product or SaaS Service that may be used to generate logs, statistics and reports regarding performance, availability, integrity and security of the Product or SaaS Service.

**13.26 “User”** means Buyer, its Affiliates and any person or software program or computer systems authorized by Buyer or any of its Affiliates to access and use the Product as permitted under this Agreement, including Contractors of Buyer or its Affiliates.

#### **Data Processing Addendum for Standard Contract for AWS Marketplace**

This Data Processing Addendum (this “Addendum”) is part of the Standard Contract for AWS Marketplace (the “Standard Contract”) between Licensor (who is the Processor) and Buyer (who is the Controller) and governs Licensor’s processing of Personal Data in its capacity as a Processor in connection with Licensor’s provision of the Services it provides pursuant to

the Standard Contract. This Addendum shall only apply if Licensor and Buyer have not entered into a separate data processing agreement or similar contractual arrangement with respect to the processing of Personal Data. All capitalized terms used but not defined in this Addendum have the meanings given to them in the Standard Contract.

## **Processing of Personal Data**

### **I. DEFINITIONS**

1. **“Controller”** means the entity that determines the purposes and means of the processing of Personal Data. “Controller” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “Business” or “Third Party,” as context requires.
2. **“Personal Data Breach”** means a confirmed breach of security of the Services that caused an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, or an event that qualifies as a reportable data breach under applicable Data Protection Law.
3. **“Processor”** means an entity that processes personal data on behalf of another entity. “Processor” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “Service Provider,” as context requires.
4. **“Sensitive Data”** means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm-Leach-Bliley Act; an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and precise geolocation.

### **II. INTERNATIONAL DATA TRANSFERS**

1. **International Data Transfer.** Before Buyer transfers Personal Data to Licensor, or permits Licensor to access Personal Data located in a jurisdiction that requires an International Data Transfer Mechanism, Buyer will notify Licensor of the relevant requirement and the parties will work together in good faith to fulfill the requirements of that International Data Transfer Mechanism. The parties will institute and comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law.

### **III. DATA PROTECTION GENERALLY**

1. **Compliance.** The parties will comply with their respective obligations under Data Protection Law and their respective privacy notices.
2. **Confidentiality.** Licensor will restrict access to Personal Data to those authorized persons who need such information to provide the Services. Such authorized persons are obligated to maintain the confidentiality of any Personal Data.
3. **Security.** Licensor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the Personal Data provided by Buyer and processed by Licensor. Such security measures will be at least as protective as the security requirements set forth in the Standard Contract. When choosing security controls, Licensor will consider the state of the art, the cost of implementation, the nature, scope, context, and purposes of Personal Data processing, and the risk to data subjects of a security incident or Personal Data Breach affecting Personal Data.
4. **Retention.** Personal Data received from Buyer will be retained only for so long as may be reasonably required in connection with Licensor's performance of the Standard Contract or as otherwise required under Data Protection Law.
5. **Cooperation.** Licensor will cooperate to the extent reasonably necessary in connection with Buyer's requests related to data protection impact assessments and consultation with supervisory authorities and for the fulfillment of Buyer's obligation to respond to requests for exercising a data subject's rights under Data Protection Law. Licensor reserves the right to charge Buyer for its reasonable costs in collecting and preparing Personal Data for transfer and for any special arrangements for making the transfer.
6. **Third Party Requests.** If Licensor receives a request from a third party in connection with any government investigation or court proceeding that Licensor believes would require it to produce any Personal Data, Licensor will inform Buyer in writing of such request and cooperate with Buyer if Buyer wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable Law.
7. **Instructions from the Buyer.** Notwithstanding anything in the Standard Contract to the contrary, Licensor will only process Personal Data in order to provide the Services to Buyer, in accordance with Buyer's written instructions, as permitted by the last sentence of Section III.8 below, or as required by applicable Law. Licensor will promptly inform Buyer if following Buyer instructions would result in a violation of Data Protection Law or where Licensor must disclose Personal Data in response to a legal obligation (unless the legal obligation prohibits Licensor from making such disclosure).
8. **Scope of Processing.** Licensor is prohibited from: (a) Selling (as such term is defined in the CCPA) Personal Data, (b) retaining, using, or disclosing Personal Data for any purpose other than for the specific business purpose of performing Buyer's documented instructions for the business purposes defined in this Addendum, including retaining, using, or disclosing the Personal Data for a commercial purpose other than performing Buyer's instructions, or (c) retaining, using, or disclosing the Personal Data outside of the direct business relationship between the parties as defined in this Agreement. Licensor certifies that it understands these restrictions. Notwithstanding the foregoing, Licensor may process Personal Data to retain or employ another person as a sub-Processor (as defined in Section III.10 below) in accordance with this Addendum, for internal use by the Licensor to improve the quality of its services (provided that Licensor does not use the Personal Data to perform services on behalf of another person), or to detect data security incidents or protect against malicious, deceptive, fraudulent or illegal activity.
9. **Sensitive Information.** Buyer will inform Licensor if Personal Data is Sensitive Data.
10. **Sub-processors.** Buyer grants Licensor general authorization, as a processor, to engage other processors (“Sub-processors”) to assist in providing the Services consistent with the Standard Contract. Licensor will make a list of such Sub-

processors accessible to Buyer prior to transferring any Personal Data to such Sub-processors. Licensor will notify Buyer of any changes to the list of Sub-processors by updating such list from time to time in order to give Buyer an opportunity to object to such changes.

**11. Sub-processor Liability.** Where Licensor engages a Sub-processor for carrying out specific processing activities on behalf of Buyer, substantially similar data protection obligations as set out in this Addendum will be imposed on that Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Law. Licensor will be liable for the acts or omissions of its Sub-processors to the same extent as Licensor would be liable if performing the services of the Sub-processor directly.

**12. Recordkeeping.** Upon a request issued by a supervisory authority for records regarding Personal Data, Licensor will cooperate to provide the supervisory authority with records related to processing activities performed on Buyer's behalf, including information on the categories of Personal Data processed and the purposes of the processing, the use of service providers with respect to such processing, any data disclosures or transfers to third parties and a general description of technical and organizational measures to protect the security of such data.

**13. Transfer of Personal Data; Appointment.** Buyer authorizes Licensor to transfer, store or process Personal Data in the United States or any other country in which Licensor or its Sub-processors maintain facilities. Buyer appoints Licensor to perform any such transfer of Personal Data to any such country and to store and process Personal Data in order to provide the Services. Licensor will conduct all such activity in compliance with the Standard Contract, this Addendum, data protection Law, any applicable International Data Transfer Mechanism and Buyer instructions.

**14. Deletion or Return.** When instructed by Buyer, Licensor will delete any Personal Data or return it to Buyer in a secure manner and delete all remaining copies of Personal Data after such return except where otherwise required under applicable Law. Licensor will relay Buyer's instructions to all Sub-processors.

**15. Breach Notification.** After becoming aware of a Personal Data Breach, Licensor will notify Buyer without undue delay of: (a) the nature of the Personal Data Breach; (b) the number and categories of data subjects and data records affected; and (c) the name and contact details for the relevant contact person at Licensor.

**16. Audits.** Upon request, Licensor will make available to Buyer all information necessary, and allow for and contribute to audits, including inspections, conducted by Buyer or another auditor mandated by Buyer, to demonstrate compliance with data protection Law. For clarity, such audits or inspections are limited to Licensor's processing of Personal Data only, not any other aspect of Licensor's business or information systems. If Buyer requires Licensor to contribute to audits or inspections that are necessary to demonstrate compliance, Buyer will provide Licensor with written notice at least 60 days in advance of such audit or inspection. Such written notice will specify the things, people, places or documents to be made available. Such written notice, and anything produced in response to it (including any derivative work product such as notes of interviews), will be considered Confidential Information and, notwithstanding anything to the contrary in the Standard Contract, will remain Confidential Information in perpetuity or the longest time allowable by applicable Law after termination of the Standard Contract. Such materials and derivative work product produced in response to Buyer's request will not be disclosed to anyone without the prior written permission of Licensor unless such disclosure is required by applicable Law. If disclosure is required by applicable Law, Buyer will give Licensor prompt written notice of that requirement and an opportunity to obtain a protective order to prohibit or restrict such disclosure except to the extent such notice is prohibited by applicable Law or order of a court or governmental agency. Buyer will make every effort to cooperate with Licensor to schedule audits or inspections at times that are convenient to Licensor. If, after reviewing Licensor's response to Buyer's audit or inspection request, Buyer requires additional audits or inspections, Buyer acknowledges and agrees that it will be solely responsible for all costs incurred in relation to such additional audits or inspections.