



GCloud Services Terms and Conditions

Between

Somerford Associates Limited

AND

XXXXXXX (Client)

Dated xx/xx/xx

Introduction

This time and materials Services Agreement ("Agreement") is between Somerford Associates ("Somerford") and xxxxxxxxxxxxxxxx ("Customer"). This Agreement defines the scope of the services ("Services") that Somerford Associates will provide to the Customer.

Project Summary

To be completed for each project

Project Conditions

- Services are performed on a "time and materials" basis. The cost set out in this Agreement is a "not to exceed" amount. Should any items require additional time to complete then an additional Agreement will be agreed by both parties.
- The Customer will provide remote access via WebEx, MS Teams or another comparable remote access solution to the Somerford Engineer in order to facilitate the delivery of offsite Services and/or troubleshooting as required.
- Every effort has been made to account for whether a particular service will be delivered offsite or onsite. However, in certain circumstances, services previously designated as "onsite" may be performed remotely (offsite) and in such case no credit for the difference in the fees associated with these different "day types" will be provided to the Customer.
- If after six months from the date of the Effective Date there remain unused/undelivered days of services, the Customer will contact Somerford Associates to discuss scheduling services for those days. Unless otherwise agreed in writing, any unused and unscheduled days of services will expire one year from the date of the signing of this SOW, at which point Somerford Associates will be under no obligation to perform any additional services under this SOW. No credit/refund of unused service days will be provided.

Requirements

Please itemise each requirement, providing a name and description for each individual work item.

Work Item Name	Work Item Description

Contacts

	Name	Email	Phone
Somerford Commercial			
Somerford Technical			
Client Management			
Client Technical			

Client Responsibilities

The work will be performed under the scope as defined in this Agreement. The Agreement is subject to the following assumptions:

The client

- will provide access to equipment and personnel (including technical resources) necessary to complete the project. These resources will be provided when they are needed in order to avoid project delays.
- will appoint a single point of contact for the duration of the project. This person will have project management responsibilities, be technically astute and familiar with change request processes as well as have the authority to expedite if necessary.
- must provide Somerford a one (1) week notice for any cancellation or change of scheduled services or they will be charged for the originally scheduled time and any applicable travel change fees.
- will provide Somerford with access to the required servers and software to complete the Agreement requirements.
- will provide the Somerford consultant(s) with either access to the Internet or access to a computer with access to the Internet as required.
- prior to the testing phase, the Customer is responsible for producing the necessary testing scenarios.
- will either provide Somerford with a client contact that has the proper administrative access to all applications and servers and will have the ability to reboot servers as necessary within twenty-four (24) hours of request or will provide Somerford with this capability.
- will ensure all systems meet the minimum system requirements.
- will ensure all systems and applications that are part of the SOW must be on supported platforms.

Amendment to the Scope

During the performance of the engagement, certain issues may arise that effectively prevent the completion of the work outlined in this Agreement within the planned time frame, such as, but not limited to, hardware or network failures or outages in the Client's environment, problems with the Client's in-house or third-party software, or the unavailability of key Client personnel. If this situation occurs, the designated Somerford Consultant will work with the Client to identify and document the scope change, its impact on the project approach, timing, fees, resources, and the quality of project results. Somerford will document this and any change in scope must be agreed to in writing prior to Somerford reengaging on the project and will require the signature of both

Somerford and the Client. Any other problems, disputes or issues arising during this engagement should be communicated as soon as possible after identification to the designated Somerford Consultant for resolution.

Fees

Somerford professional services rates are as per the G-Cloud 15 price list. All prices are quoted exclusive of VAT

Payment

Invoices are to be paid within 30 days from the invoice date.

Duration

Somerford estimates that the Agreement will require the following number of professional services days to complete.

Quote

x days of professional services * £x's

Data Processing

Subject Matter of Processing

Personal and Commercially sensitive Data relating to [ADD DETAILS] which Somerford may process in carrying out its legitimate business interests and obligations under this SoW.

Duration of Processing

For the later of Somerford's fulfilment of its obligations to the Customer or termination of this SoW.

Nature of Processing

Collection, and such organisation, adaptation, storage, retrieval, consultation, use, disclosure, making available, restriction, erasure and destruction as is necessary for the fulfilment of this SoW.

Purpose

Carrying out Somerford's legitimate business interests and obligations to the Customer pursuant to this SoW.

Data Subject Types

Customer employees, economic and financial documents, system logs or data provided in confidence by customers for the fulfilment of this SoW.

MASTER TERMS

These Master Terms are executed as of **Select Date** (the “**Effective Date**”), between OneSpan North America Inc., with registered offices at 121 West Wacker, Suite 2050, Chicago, IL 60601 (“**Supplier**”) and **Enter Customer full legal name** with registered offices at **Enter Customer address** (“**Customer**”), and govern Customer’s purchase of hardware appliances and devices (“**Hardware**”), software (provided on premise and/or as a service “**SaaS**”) and related documentation (“**Software**”) (collectively referred to as “**Products**”) and related maintenance, support, or professional services, (collectively referred to as “**Services**”) from Supplier.

1. Commercial Conditions

(a) **Order Documents.** The Customer will place all orders for Products and Services via: (i) a signed quote or order form referencing these Master Terms (“**Order Form**”); or (ii) a purchase order or other written communication from Customer that is accepted by Supplier under an order confirmation document (an “**Order Confirmation**”) referencing these Master Terms. The Order Form and/or Order Confirmation are “**Order Documents**”. These Master Terms together with its applicable schedules and Order Document constitute the “**Contract**”.

(b) **Schedules.** These Master Terms incorporate the schedules attached hereto that are applicable to Customer’s purchase of Products and Services (the “**Schedule**”).

(c) **Payment.** Customer will pay Product and Services fees (“**Fees**”) in the currency set forth in the Order Document within thirty (30) days of invoice date. Supplier reserves the right to require pre-payment, down payment, standby letter of credit, or bank guarantee at any time. Customer’s non-use of the Products or Services is not a basis for refusing to pay any Fees. Any usage of the Products and Services in excess of the amounts purchased in the applicable Order Document are subject to additional Fees.

(d) **Late Payment; Non-Payment.** If the Customer fails to pay any Fees due, Supplier may (i) immediately suspend the delivery of any Product or Service until all amounts due are paid; (ii) request immediate payment or pre-payment for Products or Services; and/or (iii) cancel, without liability to Supplier, any or all Contracts. All Fees due and unpaid shall bear default interest from the invoice date at the higher rate of one and a half percent (1.5%) per month or the applicable legal rate.

(e) **Taxes and Charges.** All Fees are exclusive of any taxes, customs duties, and similar assessments in any jurisdiction based on gross revenue, delivery, possession, and/or use of the Products or Services, or the execution or performance of a Contract, except on net income, net worth or franchise taxes assessed on Supplier.

Customer will pay all duties and taxes in any form such as service taxes, excise duties, VAT, GST, WHT, and similar charges and, when applicable, provide Supplier with an appropriate certificate of exemption.

2. Disclaimer of Warranties

EXCEPT AS EXPRESSLY SET FORTH HEREIN OR IN THE APPLICABLE SCHEDULE, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, ALL PRODUCTS AND SERVICES ARE PROVIDED “AS IS” AND ALL WARRANTIES, CONDITIONS, REPRESENTATIONS, AND GUARANTEES WITH RESPECT TO THE PRODUCTS OR SERVICES, WHETHER EXPRESS, IMPLIED, ARISING BY LAW, CUSTOM, PRIOR ORAL OR WRITTEN STATEMENTS BY SUPPLIER OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF CONDITION OR OF MERCHANTABILITY, INTEGRITY OF DATA, SATISFACTORY QUALITY, FITNESS FOR PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT) ARE HEREBY OVERRIDDEN, EXCLUDED, AND DISCLAIMED TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

3. Limitation of Liability

NEITHER PARTY NOR ITS AFFILIATES, LICENSORS, OR SUPPLIERS SHALL, UNDER ANY CIRCUMSTANCES, HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY INDIRECT, RELIANCE, INCIDENTAL, PUNITIVE, EXEMPLARY, SPECIAL OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOSS OF REVENUE OR PROFITS, LOST OR DAMAGED DATA, SERVICE DOWNTIME, CHANGE IN IP ADDRESS, BUSINESS INTERRUPTION, REPLACEMENT OR RECOVERY COSTS OR OTHER COMMERCIAL OR ECONOMIC LOSS, EVEN IF THE PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE, AND WHETHER ARISING OUT OF BREACH OR FAILURE OF AN EXPRESS OR IMPLIED WARRANTY, BREACH OF CONTRACT, MISREPRESENTATION, NEGLIGENCE, STRICT LIABILITY IN TORT, OR OTHERWISE.

EXCEPT AS SPECIFICALLY STATED IN SECTION 5 (INDEMNITY), OR FOR DAMAGES RESULTING FROM (i) SUPPLIER’S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, (ii) SUPPLIER’S BREACH OF ITS OBLIGATIONS UNDER SECTION 7 (CONFIDENTIALITY), OR (iii) DEATH OR PERSONAL INJURY CAUSED BY SUPPLIER, IN NO EVENT WILL THE AGGREGATE LIABILITY OF SUPPLIER AND ITS AFFILIATES AND LICENSORS FOR ANY AND ALL CLAIMS, ACTIONS OR PROCEEDINGS BASED ON BREACH OR REPUDIATION OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, TORT, STATUTORY DUTY, OR OTHERWISE ARISING OUT OF OR IN CONNECTION WITH A CONTRACT EXCEED THE TOTAL AMOUNT ACTUALLY PAID BY CUSTOMER FOR THE SPECIFIC PRODUCT OR SERVICE THAT DIRECTLY CAUSED THE DAMAGE IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE CLAIM.

4. Force Majeure

If Supplier is prevented or delayed in the performance of any obligation in a Contract by any event beyond its reasonable control (including, but not limited to, strikes, accidents, fires, explosions, earthquakes, pandemic, the inability to procure materials from the usual sources of supply, or act, requisition, or order of any governmental authority restricting or prohibiting the supply of the Products or Services or making such supply commercially unreasonable), Supplier shall be excused from performance or punctual performance for so long as the cause of prevention or delay continues.

5. Indemnity

If any claim, proceeding, or action is brought against Customer by a third party claiming that the Products infringe a patent, trade secret or copyright, Supplier will indemnify and defend Customer at Supplier's expense and, subject to this Section pay the liabilities, damages, costs, and reasonable attorney's fees finally awarded against Customer by a court of competent jurisdiction or agreed upon by Supplier in a settlement in the infringement action, but only if (i) Customer notifies Supplier promptly in writing that the claim or demand was received by Customer or may be asserted, (ii) Supplier has sole control over the defense of the claim and any negotiation for its settlement or compromise, and (iii) Customer takes no action that, in Supplier's judgment, is contrary to Supplier's interests.

If a claim may or has been asserted, Supplier will, at its option and expense, (i) procure the right to continue using the Products, (ii) replace or modify the Products to eliminate the infringement while providing functionally equivalent performance, or (iii) terminate the use of the Products and (a) for Products provided on a perpetual basis: refund the Fees paid for such Products, less depreciation based on a twenty-four (24) month straight-line depreciation schedule, or (b) for Products licensed on a term basis: refund on a pro rata basis Fees paid for such Products.

Supplier will have no indemnity obligation to Customer if the patent or copyright infringement claim results from (i) a correction or modification of the Product not provided by Supplier, (ii) the failure to promptly install a patch, fix, or update, if available, (iii) the combination, operation, or use of the Products with products, services, software programs, hardware, data, equipment, or other items or products not supplied by Supplier; (iv) Supplier's compliance with Customer's configuration, designs, specifications, or instructions; or (v) any claim resulting from or related to the Data (as defined in the SaaS Schedule). Customer acknowledges and agrees that this Section sets forth Customer's exclusive remedy and Supplier's exclusive liability for any actual or alleged infringement or misappropriation claim related to the Products.

6. Insurance

Supplier shall maintain throughout the Term, at its expense, insurance coverage in commercially reasonable amounts, duration and types relevant to its business and operations.

7. Confidential Information

(a) **"Confidential Information"** means all information disclosed by either party (as **"Discloser"**) to the other party (a **"Recipient"**) directly or indirectly in any form such as written, oral or visual, in machine-readable or other tangible form, relating to its business. Confidential Information includes but is not limited to patents, trade secrets, research and development plans, current and future products, product pricing, customers lists, markets, business plans, financial data, contractual terms, documentation, records, studies, reports, know-how, test results, software, and software source code. Excluded is information: (i) known to Recipient before receiving it from Discloser; (ii) independently developed by Recipient without use of or reference to any Confidential Information of Discloser; (iii) acquired by Recipient from another source not otherwise subject to confidentiality obligations; or (iv) in the public domain through no fault or action of Recipient.

(b) **Protection of Confidential Information.** Recipient shall use no less than reasonable means to prevent the disclosure and to protect the confidentiality of the Confidential Information of Discloser. Recipient shall not knowingly disclose Confidential Information to any third party, except on a need-to-know basis and for purposes of a Contract, and under confidentiality obligations at least as restrictive as contained herein. Each party may disclose Confidential Information to its Affiliates in the administration or performance of a Contract. While maintaining the confidentiality of Customer's Confidential Information, Customer permits Supplier to gather and use Products or Services usage data for business intelligence purposes, including for Supplier to develop new features or functionalities that will benefit users of the Products or Services. **"Affiliate"** means any entity that controls, is controlled by or is under common control with a party to this Contract, where control means, for the purposes of this definition, with respect to any entity, the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity, whether through the ownership of voting securities (or other ownership interest), by contract or otherwise.

(c) **Required Disclosure.** If Recipient is required by law to disclose Discloser's Confidential Information or the terms of a Contract other than as permitted under this Section, Recipient will give prompt written notice to Discloser before making the disclosure, unless prevented by the legal or administrative process, and will reasonably assist the Discloser to obtain when available an order protecting the Confidential Information from public disclosure.

(d) **Remedies.** Recipient acknowledges that any actual or threatened breach of this Section may cause irreparable, non-monetary injury to the Discloser. Accordingly, the Discloser is entitled to seek injunctive relief in addition to all remedies available at law and/or in equity, to prevent or mitigate any breaches of these Master Terms or any Contract, or any damages that may otherwise result from those breaches.

8. Data Protection

Supplier and its affiliates may collect, use, process, transfer, and store Personal Data in the form and manner described in <https://www.onespan.com/privacy-center> and subject to applicable data protection laws.

Customer represents and warrants that Customer (i) will transfer to Supplier only Personal Data necessary for the performance of the Contract, (ii)

has provided notice to and obtained all necessary consents of the data subject or has appropriate legal basis for the processing of personal data in accordance with applicable laws for the transfer and use of Personal Data to Supplier; and (iii) maintains security and safety measures in the transfer and access to Supplier of Personal Data (including de-identification of client or end-user related information unless transfer is necessary in the Contract).

Supplier takes reasonable and appropriate measures to safeguard the confidentiality and security of Personal Data and to prevent its unauthorized use or disclosure. Customer can request access to Personal Data that Supplier maintains. To protect privacy of Personal Data, Supplier will take reasonable steps to verify Customer's or the requesting person's identity before granting access to or making changes to Personal Data.

9. Ownership and Suggestions

(a) **Ownership.** All trademarks and service marks (registered or not), patents, copyrights, trade secrets, and all other intellectual property and proprietary rights in and to the Products and/or Services including in any copy, translation, localization, adaptation, improvement, development, or derivative thereof ("**Intellectual Property**"), are and will remain the exclusive property of Supplier, its affiliates or its licensors, whether or not specifically recognized or perfected under applicable law. Other than as expressly granted herein, Customer shall not acquire any rights to or take any action prejudicial to Supplier's Intellectual Property rights. Customer waives and will not exercise any rights it may have in the Intellectual Property, and shall cause its employees and contractors to do the same. To the extent such waiver is invalid under the law, Customer grants to Supplier, its affiliates and licensors the exclusive, perpetual, irrevocable, worldwide and royalty free right to use, market, and modify any such items without any obligation of attribution or consent, and shall cause its employees and contractors to do the same.

Customer may not use the Supplier trademarks without Supplier's prior written consent. Customer shall not alter or remove any Supplier trademarks applied to the Products and/or Services. Customer shall not challenge or assist others to challenge the Supplier trademarks or the registration thereof or attempt to register any trademarks, service marks or trade names confusingly similar to those of Supplier, its affiliates or its licensors. Any authorized use by Customer of the Supplier trademarks shall inure to the benefit of Supplier.

(b) **Suggestions.** To the extent Customer provides or otherwise communicates any suggestions, enhancement requests, recommendations or otherwise provides feedback on the Products and Services (collectively, "**Suggestions**"), Customer hereby grants Supplier a royalty-free, worldwide, transferable, sub-licensable, irrevocable, perpetual, unrestricted license to use and/or incorporate the Suggestions and all underlying ideas contained in the Comments into the Service (or other product offerings) and create any derivative works thereof.

10. Governing Law

This Contract shall be governed by and interpreted in accordance with the laws of (i) Ontario if Customer is located in Canada, (ii) Switzerland, if Customer is located in Europe, Middle East, or Asia Pacific, (iii) England if Customer is located in the United Kingdom, or (iv) the State of Delaware, United States, if Customer is not located in those countries listed under (i), (ii) or (iii). The parties exclude from this Contract the application of the United Nations Convention on Contracts for the International Sale of Goods. Supplier may seek injunctive relief or file for collection of debt in courts with appropriate jurisdiction as may be necessary.

11. Compliance with Laws

Customer shall, at its expense, comply with all laws, regulations, authorizations, and any legal requirements in its jurisdiction that apply to its performance of the Contract and to the use, distribution, or resale of the Products and/or Services.

Supplier's provision of the Products, Services, technical information, and related materials is subject to EU and US export control and trade sanctions laws and regulations ("**Trade Controls**"). Customer acknowledges the application of such Trade Controls and agrees to (i) comply strictly with the legal requirements established under the Trade Controls, (ii) cooperate with Supplier in any official or unofficial audit, inspection or investigation that relates to the Trade Controls, and (iii) not export, re-export, distribute, use or otherwise transfer, directly or indirectly, the Products, Services, any technical information or materials, or any related product thereof to any destination, company or person restricted or prohibited by the Trade Controls, unless authorized or permitted under applicable Trade Controls and unless Customer has obtained prior written authorization from Supplier and the applicable governmental organization.

Customer agrees that Supplier's non-performance of any obligation herein due to Supplier's adherence to Trade Controls or compliance with laws will not constitute a breach of the Contract.

12. Customer's Warranties

Customer is responsible for the proper and authorized use of the Products and Services. Customer represents and warrants that: (i) it will not use or allow use of the Products and/or Services for or in connection with any illegal or unlawful purpose or activity where the Products and/or Services are made accessible or available; and (ii) it will not use or deal with the Products and/or Services in any way prejudicial to Supplier or in any way that will expose Supplier or any of its directors, officers, or employees to liability including without limitation under environmental, securities, anti-corruption, anti-gambling or other penal laws, or Trade Controls. Customer agrees to take all measures to mitigate any damages hereunder.

13. Third Party Components

Products may include features provided by third parties for use within the applicable Product ("**Third Party Components**"). Some Third Party Components are subject to additional terms mandated by the third party provider and are available for review at <https://www.onespan.com/third-party-terms> and are incorporated into this Contract.

14. Term and Termination

(a) **Term.** The Contract is effective on the Effective Date and continues until it expires or is terminated as indicated herein.

Unless otherwise indicated in an applicable Schedule the Contract continues until the term or subscription of all Products and Services ordered under the applicable Order Document expire or until all Order Documents otherwise terminate as set forth herein (the “**Term**”).

“**Start Date**” means the subscription or term start date specified for the applicable Product or Service on the Order Document.

“**End Date**” means the subscription or term expiration date specified for the applicable Product or Service on the Order Document.

“**Order Date**” means the date located in a date field on an Order Document, typically is the date an Order Document is generated.

Due to the account provisioning process, it may be necessary to change the Start Date of a Product to a later date than stated in the signed Order Form or listed in Customer PO. The parties agree that (i) Supplier may issue an Order Confirmation after receipt of a signed Order Form or PO with updated Product Start Dates, (ii) the Order Confirmation shall take precedence over the signed Order Document or PO with respect to the Start and End Dates; (iii) the Start and End Dates on the Order Confirmation shall only be later than those on the signed Order Form.

(b) **Automatic Renewal.** Orders for Products and Services that are provided on a subscription or term basis such as SaaS, Software licenses limited in time, and maintenance and support, will automatically renew for renewal terms of twelve (12) months (the “**Renewal Term**”) unless either party cancels the upcoming Order Document Renewal Term by providing notice at least sixty (60) days prior to the End Date. Unless otherwise indicated in the Order Document: (i) the terms and conditions applicable to Renewal Term(s) are the most recently published terms and conditions, and (ii) OneSpan reserves the right to increase the Product price for any subsequent Renewal Term upon ninety (90) days prior notice, but in no case will the increase be more than three percent (3%).

(c) **Termination.** Without prejudice to any of the parties’ rights and obligations, either party may terminate the Contract by written notice to the other party (i) if the other party is dissolved, declared bankrupt, granted suspension of payments, moratorium, has a receiver, administrator or manager appointed over the whole or part of its assets or business, (ii) if the business of the other party has been discontinued, or (iii) for material breach of a Contract and such breach is incapable of cure; or being capable of cure, remains uncured for 30 days after the breaching party receives detailed written notice thereof.

(d) **Effect of Expiration or Termination.** Upon the expiration or termination of a Contract for any reason, all rights granted to Customer will cease and Customer will delete and destroy all copies of any Software including, but not limited to, any software embedded in or installed on devices and all activation codes. Termination of any Contract does not relieve payment obligations due prior to termination, or other than for Customer’s termination for cause, for any current Term or future committed Term, and does not give either party any right to compensation, reimbursement, refund, credit, or any other damages or losses.

(e) **Survival.** The terms, conditions and warranties contained in the Contract which by their nature and context are intended to survive the performance hereof shall so survive the expiration or termination of the Contract.

15. Audit

(a) **Supplier Audit.** Supplier shall be entitled, at its expense and with reasonable notice to Customer, to perform an audit at Customer's headquarters or any other relevant premises to verify Customer's conformity with its obligations.

(b) **Customer Audit.**

Supplier shall maintain records and supporting documentation of (i) its performance of its obligations under this Contract, and (ii) assessments, certifications and/or audits related to security of its SaaS and data protection (“**Records**”).

Supplier shall, upon Customer’s thirty (30) days written notice, allow Customer or Customer’s independent auditor to access the Records as may be reasonably required by Customer in order to: (i) fulfil a lawful request by a regulatory body of Customer; or (ii) undertake verifications of the accuracy of the Fees; (an “**Audit**”).

Customer shall not exercise its rights of Audit more than once a year during the Term and shall ensure that the conduct of the Audit does not disrupt Supplier’s operations or delay the provision of the SaaS by Supplier. No access will be given to the Supplier’s or its subcontractors premises unless it is lawfully requested by a regulatory body of Customer.

Subject to the above conditions and in compliance with the obligations of confidentiality and security in this Contract and any obligations of confidentiality or security Supplier has towards other customers, Supplier shall provide Customer or Customer’s independent auditor with reasonable co-operation and assistance in relation to the Audit.

The Audit shall be at Customer’s cost and expenses and any efforts of Supplier beyond eight (8) hours per year to provide such assistance as contemplated in this section will be charged to Customer on time and material basis at a then applicable Professional Services Fees rate.

16. Resale of Products or Services

For the purpose of this Section: (i) “**Customer Agreement**” means the agreement and applicable schedules that govern the End Customer’s use of the Products and Services provided by Reseller to End Customers as set forth at <https://www.onespan.com/master-terms>. The Customer Agreement may be amended from time to time by Supplier; (ii) “**End Customer**” means the person or entity who enters into an agreement with Supplier to use the Product or Service as facilitated by Reseller; and (iii) “**Reseller**” means a company appointed by Supplier to act, as a non-exclusive reseller of

the Products and Services indicated on the applicable Order Document.

Provided that Reseller has received Supplier's prior written consent in each instance, Reseller may obtain certain Products or Services from Supplier for the purpose of reselling the Products and Services to End Customers, provided that: (i) at the time of its submittal of an Order Document to Supplier for resale of Products or Services to the End Customer, Reseller ensures that the End Customer has agreed to the Customer Agreement; (ii) Reseller does not install or use any of the Products prior to reselling the Products; (iii) Reseller remains liable for all payments to Supplier regardless of when or if the End Customer receives payment from the third party; (iv) Reseller shall not make any representations in connection with the Products or Services other than those set forth in these Master Terms or the applicable Schedule; (v) Reseller shall indemnify Supplier against any damage, loss, liability or expense that Supplier may incur as a result of any representation or commitment made by Reseller which is in addition to or in lieu of those set forth in these Master Terms and the applicable Schedule; and (vi) any reference to "Customer" in these Master Terms shall mean "Reseller" for the purposes of resales under this Section.

17. Non-Production Use

Notwithstanding anything in this Contract, if Customer is participating in free of charge, sandbox, proof of concept, trial, testing, development or other non-production use ("**Non-Production Use**") of OneSpan Products or Services as indicated in an Order Document or via an online website, OneSpan will make the Products and/or Services available to Customer until the earlier of (a) the end of the limited term Non-Production Use period as indicated in the Contract, (b) the start date of any Contract executed by Customer for productive use of the Product or Service, or (c) cessation or suspension of the Product or Service at Supplier's option. Any Data produced from Non-Production Use of the Product and/or Service or provided to OneSpan during the Non-Production Use is not recoverable or available upon the expiration or termination of the aforementioned Non-Production Use period. **NOTWITHSTANDING ANYTHING IN THIS CONTRACT, THE NON-PRODUCTION USE PRODUCTS AND/OR SERVICES ARE PROVIDED "AS-IS", WITHOUT ANY WARRANTY, SERVICE LEVELS, LIABILITY OR INDEMNITY OBLIGATIONS PROVIDED BY ONESPAN.**

18. US Government Rights

Supplier's Software is commercial computer software (as defined in Federal Acquisition Regulation ("FAR") 2.101 for civilian agency purchases and Department of Defense ("DOD") FAR Supplement ("DFARS") 252.227-7014(a)(1) for defense agency purchases) and Supplier Services are commercial items. If the Software is licensed or Services acquired by or on behalf of a civilian agency, Supplier provides the Software, its Documentation, and any other technical data subject to this Contract consistent with FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data). If Software is licensed or Services acquired by or on behalf of any DOD agency, Supplier provides the Software, its Documentation, and any other technical data subject to this Contract consistent with DFARS 227.7202-3. If this is a DOD prime contract or DOD subcontract, the DOD agency Customer may acquire additional rights in technical data under DFARS 252.227- 7015(b). This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

19. Miscellaneous

The Contract constitutes the entire agreement between the parties with respect to the subject matter therein and supersedes any prior proposal, representation, or written agreement, except if specifically agreed otherwise. Any modification or waiver of any provision of the Contract is binding only if made in writing signed by both parties. Other than as expressly stated that it supersedes a specifically identified section of the Contract, any inconsistency in any documents relating to the Contract shall be resolved by giving precedence in the following order: (i) the applicable Schedule (including the exhibits attached thereto); (ii) these Master Terms; (iii) the applicable statement of work; and (iv) the applicable Order Document.

Except as otherwise stated in the applicable Schedule, all notices or approvals must be given in writing to Supplier at the address indicated in the Contract. Notwithstanding the foregoing, Supplier may give Customer notice electronically. Electronic notice to Customer is deemed given when transmitted to an email address furnished by Customer to Supplier.

Customer may not assign or transfer its rights or duties in whole or in part to a third party without written consent of Supplier.

Notwithstanding the foregoing, either party may assign its rights and/or obligations hereunder with notice to the other party, to (i) a related party, or (ii) an unrelated party pursuant to an assignment, transfer and conveyance of substantially all or a portion of its assets, a merger, consolidation or other corporate reorganization. Any assignment in violation of this Section is void and of no force or effect.

If a court declares any provision of the Contract as unlawful, void, or for any reason unenforceable, such declaration shall not affect the validity or enforceability of the remaining provisions.

Customer's purchase orders, online procurement and invoicing portals are for Customer's convenience only and do not add to, alter, or otherwise amend the Contract.

The Contract, Schedules, and all documents and materials related to the Products and Services have been drafted in English. Any translations to any other language shall be only for convenience or for purposes of making any necessary filings. The English version of the Contract and/or any related document or material shall be controlling in all respects and shall prevail in case of any inconsistencies with any translated version.

Le Contrat, les Annexes, ainsi que tous les documents et contenu relatifs aux Produits et services ont été rédigés en anglais. Toute traduction dans une autre langue n'est faite qu'à des fins de commodité ou aux fins du dépôt de tout document, si nécessaire. La version anglaise du Contrat et / ou de tout document ou contenu fait foi, à tous égards, et prévaut en cas de contradiction avec toute version traduite.

A Contract may be executed by means of electronic signature, or in any number of counterparts, where all such counterparts taken together will be

deemed to constitute one and the same instrument. A signed or e-signed copy of a Contract delivered by facsimile, e-mail, or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed Contract.

Attachments:

Attachment A: SaaS Subscription Schedule

IN WITNESS WHEREOF, the parties cause this Contract to be executed by their duly authorized representatives identified below.

OneSpan North America Inc.

customer

BY: _____

BY: _____

NAME: _____

NAME: _____

TITLE: _____

TITLE: _____

DATE: _____

DATE: _____

ATTACHMENT A: SaaS SUBSCRIPTION SCHEDULE

1. Definitions

“**Account**” means a unique account that may be established by Supplier for Customer’s use.

“**Administrator**” means Customer’s employee(s) or authorized agent(s) designated as the Customer contact for management and support of the Service.

“**Data**” means any data transmitted or provided to Supplier by or on behalf of Customer, or Users in its use of the Service.

“**Documentation**” means Supplier’s then-current, generally available written product guides and user manuals for the Service found at <https://community.onespan.com/documentation>, as may be updated by Supplier from time to time; but excluding any third party information.

“**Malicious Code**” means viruses, spiders, worms, time bombs, trojan horses and other harmful or malicious code, instructions, files, scripts, agents or programs or any other code intended to cause harm or disruption to computer systems.

“**Personal Data**” has the meaning given to it in the Master Terms.

“**SaaS Service**” means the Software as a Service (“SaaS”) as described in this Schedule, the OneSpan SaaS Service Descriptions found at www.onespan.com/saas-service-descriptions, and the applicable Order Document.

“**Service Levels**” mean the service level availability standards specified at www.onespan.com/onespan-saas-sla.

“**Service Term**” means the subscription term applicable to the Service which begins on the Start Date and ends on the End Date (both as defined in the Master Terms).

“**Support Service**” means telephone help desk or email support available to Customer as described in Attachment A: SaaS Support.

“**System**” means the Supplier website, the computer equipment including the servers, software, and other technology, used by Supplier to provide the SaaS Service. System does not include Customer or third party provided servers, devices or networks used to access the SaaS Service.

“**Transaction**” has the meaning given to the applicable SaaS Service in the OneSpan SaaS Service Descriptions at www.onespan.com/saas-service-descriptions.

“**Users**” means individuals who are authorized by Customer to use the SaaS Service to process Transactions.

2. Service Terms

2.1. Non-Exclusive Right to Use. Subject to this Contract, the Documentation, and the Service Use Guidelines and Service Conditions found at www.onespan.com/saas-service-use-guidelines-and-conditions, Supplier makes the SaaS Service available to Customer via the Internet during the Service Term on a non-exclusive, subscription basis. Customer may grant access to the SaaS Service to its Users.

2.2 Account Creation; Access. Upon execution of the Order Document, Supplier may establish an Account. Data is automatically stored within the data center Supplier deems optimal if not otherwise specified in the Order Document. The Administrator shall be responsible for administering the Account, including the assignment and maintenance of usernames and passwords. Customer (i) remains responsible for any access to the SaaS Service through the Account, (ii) is obligated to protect and not to disclose to third parties the usernames and passwords or any other form of access credentials linked to its Account, and, (iii) shall take reasonable steps to ensure that each User abides by the terms and conditions herein. If Customer becomes aware of any suspected or actual violation of the SaaS Service and/or System, abuse, unauthorized use or access, SaaS Service vulnerability, security incident, confidentiality or privacy breach or potential or confirmed compromise of its access credentials, then Customer shall promptly notify Supplier customer support.

2.3 Rights in Data. As between Customer and Supplier, Customer owns all Data. Customer hereby grants to Supplier a non-exclusive, worldwide, sub-licensable right to use the Data to the extent necessary to perform the SaaS Service or as expressly permitted by Customer in this Contract or otherwise in writing.

3. Provision of the Service

Supplier shall use commercially reasonable efforts to make the SaaS Service available to Customer pursuant to this Schedule on a 24/7 basis in accordance with the Service Levels. Nothing contained herein shall limit Supplier’s right to grant access or otherwise distribute or make available the SaaS Service, in whole or in part, to any third party. Supplier shall provide technical support to two (2) Administrators responsible for Customer side support and the coordination of technical requests for the use of the SaaS Service, and provide Professional Services, if any, purchased by Customer. Changes related to Customer’s Administrators may be notified to Supplier in writing. Customer will be solely responsible for providing all support to Users.

4. Data Security

Supplier has implemented administrative, technical and physical safeguards to protect the security, confidentiality and integrity of the Data in its possession set out at www.onespan.com/privacy-and-security-terms. Without limiting the above, Supplier shall not: (i) modify the Data; or (ii) disclose the Data to third parties, except as necessary to perform the SaaS Service, or as expressly permitted by Customer in this Schedule or otherwise in writing. If this Schedule is terminated, Supplier may delete Customer’s Data from the SaaS Service after the termination or expiration

of this Schedule or upon Customer's earlier written request.

5. Use by Affiliates.

Customer may: (a) use the SaaS Service in connection with its Affiliate's business within the limitations applicable to Customer; or (b) allow one or more of its Affiliates access to the SaaS Service solely to the same extent as granted to Customer in this Contract, provided Customer is authorized to bind such Affiliate. Customer shall notify Supplier of Customer's Affiliate's intent to use the SaaS Service at least thirty (30) days prior to permitting access. Customer shall ensure that each of its Affiliates using the SaaS Service receives a copy of, and complies with this Contract. If Affiliate and Supplier enter into a separate Order Document for Affiliate's use of the SaaS Service, then Affiliate agrees to be bound by the terms of this Contract as if it were an original party hereto. Customer shall remain liable to Supplier for any breach of this Contract by its Affiliates.

6. Representations and Warranties

6.1. Supplier's Warranties. Supplier warrants that (i) the SaaS Service will materially conform to the Documentation, and (ii) it shall be responsible for any breach of this Contract by its subcontractors.

6.2. Customer's Warranties. Customer warrants that: (i) it has not falsely identified itself nor provided any false information to gain access to and use of the SaaS Service and Supplier's Confidential Information; (ii) it has obtained the appropriate legal basis for processing of personal data or all necessary consents from relevant individuals in accordance with applicable laws in order to provide the Data to Supplier and process the Data with or through the SaaS Service in the manner described in this Schedule; (iii) it will not transfer to Supplier nor store any protected health information (as defined under the HIPAA Administrative Simplification Regulations at: 45 C.F.R. § 160.103) within the SaaS Service, unless explicitly permitted in the applicable Order Document signed by both parties.

6.3 In case of a breach of the warranty set forth above or any other duty related to quality, Supplier will, at its option and at no additional charge to Customer, correct the non-conforming SaaS Service, and in the event Supplier is unable to correct such non-conformance after good-faith efforts, Supplier shall refund Customer amounts paid attributable to the non-conforming SaaS Service from the date Supplier received such notice. Customer acknowledges and agrees that this Section sets forth Customer's exclusive remedy and Supplier exclusive liability for any breach of warranty or other duty related to the quality of the Service.

7. Termination; Effect of Termination

In addition to the term and termination provisions of the Master Terms, the following terms shall apply:

7.1 Termination for Convenience. Subject to Section 7.2, Customer may terminate any Service Term for convenience with thirty (30) days notice by notifying Supplier in writing of its desire to terminate the SaaS Service. Termination of the Service Term is effective on the date Customer specifies in such notice.

7.2 Effect of Expiration; Termination. The SaaS Service will terminate as of the effective date of the termination of the Contract or Service Term. Termination pursuant to Section 7.1 (Termination for Convenience) or non-renewal of any Order Document shall not relieve Customer of its obligation to pay any fees accrued or payable for the current Service Term or any future committed Service Term. Termination of the Contract or a Service Term will not prejudice or affect any right of action or remedy which will have accrued to Supplier up to and including the effective date of termination of the Contract or Service Term. For thirty (30) days following the termination or expiration of an Order Document, Customer may retrieve Data and delete stored copies.

Exhibits:

Exhibit A: Data Privacy and Security

Exhibit B: OneSpan SaaS Service Descriptions

Exhibit C: OneSpan SaaS Service Level Availability

Exhibit D: SaaS Support

Exhibit E: Service Use Guidelines and Conditions

EXHIBIT A: DATA PRIVACY AND SECURITY

1. Definitions.

“Personal Data” has the meaning given to it in the Master Terms.

“Personnel” refers to Supplier’s employees and consultants having access to Data or systems used to provide the SaaS Service and SaaS related Support Services under this Contract.

2. Generalities. Supplier shall maintain a comprehensive information security program designed to protect the security and confidentiality of Data and protect against any reasonably anticipated threats or hazards to the security or integrity of such Data.

3. Information Security Requirements. Supplier shall comply with the following security measures with regard to its production environment:

3.1. Administrative Safeguards.

- 3.1.1. Information Security Policies. Supplier shall have in place a comprehensive information security policy framework, including but not limited to policies and standards (herein collectively referred to as “Security Policies”), aligned with industry standard practices, as applicable. Such Security Policies shall address matters of information security and meet reasonably relevant/applicable statutory, regulatory and contractual requirements and have, as applicable, supporting guidelines, processes and procedures in place that set forth how Supplier will meet its security commitments. Security Policies shall include appropriate administrative, technological and physical safeguards to: (i) protect against threats to the security and confidentiality of Data, including unauthorized use, access or disclosure; (ii) ensure a consistent level of protection for Data during both normal operations and extraordinary circumstances, such as when Supplier is operating under a business continuity or disaster scenario; (iii) limit access to Data to those with a “need to know”; and (iv) ensure the secure disposal of Data. Security Policies shall be approved by senior management, communicated to Personnel and reviewed on an annual basis to ensure accuracy and completeness, and to take into account changing standards and evolving threats and hazards. Security Policies shall have provisions for disciplinary measures in case of violation.
- 3.1.2. Confidentiality. Personnel, contractors and consultants shall be subject to obligations of confidentiality which meet the intent of those found in this Contract.
- 3.1.3. Personnel security. Personnel shall have clearly defined job descriptions that include security requirements and responsibilities and such job descriptions shall be reviewed periodically to ensure their accuracy and completeness. Personnel shall undergo a background check to the extent permitted by applicable law, which includes, but is not limited to, identity verification, a criminal record check, past employment verification, education records verification, reference checks, as well as screening against the Office of Foreign Assets Controls of the U.S. Department of the Treasury’s “Specially Designated Nationals List”. Personnel shall sign a non-disclosure agreement. Personnel shall also, on a yearly basis, sign a “Privileged User Agreement” or similar form, and acknowledge the Company’s Code of Conduct. Personnel shall attend Code of Conduct training and Information Security and Privacy Awareness sessions on an annual basis.
- 3.1.4. Access control. Supplier shall maintain procedures and controls to authenticate and limit access to the systems used to provide the SaaS Service to authorized individuals. Access to such systems shall be granted on a need-to-know basis, applying the least privilege principle, as applicable. Personnel with administrative privileges shall be required to use multifactor authentication in order to get access to such systems. Personnel shall not access or view any Data unless required to provide the SaaS Services under the Contract. Access shall be removed promptly upon termination, or upon position change, as required.
- 3.1.5. Risk management. Supplier shall have in place a process to and conduct regular and comprehensive assessments of reasonably foreseeable internal and external risks and vulnerabilities to the confidentiality, integrity and availability of Data that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such Data, and design and implement safeguards to reduce these risks and vulnerabilities to a reasonable and appropriate level.
- 3.1.6. Change management. Supplier shall have in place a formalized change management process which requires the identification, documentation, testing, approval and post-implementation review of application and infrastructure changes that may impact system security, stability, availability or otherwise have an adverse effect on the SaaS Service. Proposed changes shall be evaluated to determine if they present a security risk and what mitigating actions must be performed. Access to production systems shall be strictly limited and developers shall not have the ability to migrate changes into the production environment.
- 3.1.7. Incident management. Supplier shall have in place an incident management framework designed to respond quickly and efficiently to all types of internal and external security and operational events that threaten the confidentiality, integrity or availability of the system used to provide the SaaS Services and any Data contained therein.
- 3.1.8. Business continuity and disaster recovery. The SaaS Service shall be designed with the resources reasonably necessary to support availability of the SaaS Services in accordance with the Service Levels, and in a way that would enable recovery within the established Recovery Time Objective (RTO) following a service interruption. Testing of necessary components shall be performed as reasonably required to ensure recoverability.
- 3.1.9. Organizational audits. At least annually during the Term, Supplier shall have, at its sole expense, a reputable qualified third party conduct a Service Organization Control (SOC) 2 assessment of the SaaS Service to assess the suitability of the design and the operating effectiveness of the controls to meet the Trust Services Principles and Criteria for Security established by CPA Canada/AICPA’s TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing

Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids). Such assessment shall reasonably cover all sites being used to provide the SaaS Service, herein referred to as an “Organizational Audit”. In addition to including a description and assessment of the controls in place, the Organizational Audit report will also include a description of organizational, operational and business controls relating to the SaaS Service, within the general framework of the type of Organizational Audit in question. Supplier shall make available to Customer a copy of the SOC 2 report summarizing the findings of such Organizational Audit, upon written request.

3.2. Technical Safeguards.

- 3.2.1. Data segregation. Supplier shall ensure that Data is stored, used, accessed and disposed of in a secure environment, and logically segregated at all times from its other clients’ data, including when operating under a business continuity or disaster recovery scenario.
- 3.2.2. System configuration. The system used to provide the SaaS Service shall be segmented into separate network zones protected by firewalls or equivalent mechanisms to mitigate the risk of unauthorized access and to stop the spread of malware infections at internal and external access points. Supplier shall maintain procedures and controls for the secure installation, configuration, operation and maintenance of information systems (e.g., workstations, servers, networks and applications), including procedures for change management, patch management and vulnerability management. System components shall be configured according to hardening guidelines and feature antivirus and intrusion detection systems, as applicable.
- 3.2.3. Application development. Supplier shall use separate environments for the purposes of development, testing, staging and production, so that any changes to infrastructure and software are developed and tested in a separate environment before being implemented into production, and to reduce risk of inadvertent changes to a production environment. Supplier shall perform code reviews and analyses of its software on a regular basis to reduce the likelihood of any vulnerability being deployed into production.
- 3.2.4. Monitoring. Supplier shall maintain procedures and controls for detecting, preventing and responding to attacks, intrusions or other systems failures, including actions to be taken in the event of suspected or detected unauthorized access to Data. Supplier shall have in place and maintain tools, including but not limited to a Security Incident and Event Management (SIEM) system, to allow for appropriate ongoing monitoring of the health and security of the SaaS Service, including the detection of possible security threats and incidents. Such tools shall monitor system availability, resource usage, security events, unauthorized system changes and unusual activity, and have automated notifications for system and security issues in real time. Monitored events shall be correlated centrally and event logs shall be reviewed regularly to allow for prompt identification of issues, for capacity planning and for appropriate action to be taken in a timely period in respect of any issues detected from such reviews.
- 3.2.5. Vulnerability management. In order to identify potential SaaS Service vulnerabilities, Supplier shall conduct vulnerability assessments on a regular basis. Such assessments shall include penetration testing of the network boundary as well as application vulnerability testing. Security patches and updates shall be applied as required according to their criticality.
- 3.2.6. Security Testing. At least annually, or aligned with delivery of major releases, and at Supplier’s sole discretion, Supplier shall retain a qualified, reputable third party to perform penetration testing of the SaaS Service and to prepare a report of its findings.
- 3.2.7. Use of encryption. Supplier shall use appropriate encryption, using industry-accepted algorithms and key lengths, to protect Data stored in the SaaS Service, or transmitted over public networks, in connection with the SaaS Services.
- 3.2.8. Use of portable storage. Unless explicitly requested by Customer or required to provide SaaS Services under this Contract, and protected by encryption, Data shall not be copied onto computer systems or media not permanently housed in secure Hosting Facilities (including laptop computers, portable storage devices or removable media such as USB disks, DVDs and tapes).
- 3.3. Physical and Environmental Safeguards. Access to areas at a Supplier site from which the SaaS Service is managed and can be accessed shall be physically restricted to authorized Personnel only, and controlled through the use of access badges. Visitors and third parties shall only be allowed to access to such Supplier work area once they have been properly identified and authorized.
- 3.4. Hosting Facilities
 - 3.4.1. Supplier shall host equipment used to provide the SaaS Services in a physically secure area with access restricted to authorized personnel, herein referred to as “Hosting Facilities”. Hosting Facilities shall have adequate physical security measures such as, but not limited to, perimeter controls which include a provision to detect unauthorized access, access logging, strong authentication, video surveillance and visitor sign-in.
 - 3.4.2. Hosting Facilities shall be reasonably protected against external/environmental threats such as fire, flood or other forms of natural or man-made disasters. Protection measures shall include controls such as smoke and fire detection alarm systems and/or automatic fire suppression systems.
 - 3.4.3. Hosting Facilities shall have protection in place for servers, network and other electronic equipment against power related problems.
 - 3.4.4. Supplier shall periodically review the physical and environmental controls to ensure they remain adequate to host the equipment used to provide the SaaS Services.
 - 3.4.5. Where any hardware or media is no longer being used to provide the SaaS Services, Supplier or its subcontractor will promptly render irrecoverable any Data on that hardware or media, as applicable.

4. Privacy Requirements

- 4.1. Access and Correction Requests. Supplier will refer to Customer all access or correction requests for Personal Information and reasonably cooperate with Customer in its response to those requests, as applicable.
- 4.2. Breach Notification and Investigation. In the event that Supplier becomes aware that the security, confidentiality or integrity of any Data has been compromised, or that such Data has been or is reasonably expected to be subject to a use or disclosure not authorized by this Contract (“Data Breach”), Supplier shall use commercially reasonable efforts to immediately, in writing, in accordance with the notice requirements set out in the Contract, but in no event more than two (2) business days (where feasible) following discovery or notification of such Data Breach, report to Customer and, if required by law or regulation, to any other party. Supplier shall also (i) promptly

investigate and conduct a reasonable analysis of the cause(s) of the Data Breach, (ii) to the extent such cause is within Supplier's control, develop and implement an appropriate plan to limit the effect and remediate the cause of the Data Breach; and (iii) reasonably cooperate with Customer in respect of any investigation and/or efforts to comply with any notification or other regulatory requirements applicable to the Data Breach. Subject to any confidentiality and/or contractual agreements Supplier may have with other parties, Supplier will give Customer any information Customer reasonably requests about the incident.

- 4.3. Privacy Coordinator. Supplier will appoint a privacy coordinator to oversee Supplier's compliance with its privacy and information security obligations under this Contract and to act as Customer's primary point of contact for privacy and information security matters. Supplier will notify Customer of the privacy coordinator's identity and contact information, upon written request.

EXHIBIT B: ONESPAN SAAS SERVICE DESCRIPTIONS

Communication Hub

1. Definitions

“Annual Commitment” means the number of annual Credits committed in the applicable Order Document.

“Credit” means the unit purchased in order to access and use Communication Hub services.

“Excess Limit Fee” means the price per Credit listed for the Product on the applicable Order Document that is charged for Credits in excess of the Annual Commitment.

“SMS OTP” means a text message containing a one-time access code, which the User must enter in order to gain access to the applicable Customer application, OneSpan Product, or other relevant application.

2. Product Information

OneSpan’s Communication Hub (the **“Communication Hub”**) is a global service allowing the use of SMS OTP to transmit information or features to registered Users.

Communication Hub uses Credits in order to access any of the possible combinations.

Communication Hub provides customers with two different environments to support their testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier’s discretion.

Production:

- Production usage of the current version of Communication Hub
- Subject to the Service Levels

Testing/Sandbox (Preview):

- Integration development and testing of the current version of Communication Hub
- Not subject to the Service Levels, security requirements or safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment
- Subject to Pricing requirements below and as indicated in the companion OneSpan Product Service description herein

3. Pricing

1. Pricing for Communication Hub is based upon Annual Commitment allocated as follows:
 1. SMS OTP: Credits based on the User’s telephone number geographic location as indicated below. For a list of Tiers see www.onespan.com/smsotp-tiers.
 1. Tier 1: one (1) Credit
 2. Tier 2: two (2) Credits
 3. Tier 3: three (3) Credits

2. Credits processed in excess of the Annual Commitment will be charged Excess Limit Fee. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
3. Unused Credits do not carry over to the next year.
4. For OneSpan Sign, Customer receives up to one percent (1%) of the SMS OTP Communication Hub Credits purchased by Customer in production environment for use in the Sandbox (Staging) environment provided free of charge. Use in excess of this amount in Sandbox (Staging) will result in Excess Limit Fees.

4. Additional Information

a. For SMS OTP the following terms apply:

- i. Customer is responsible for providing correct phone number for applicable User. SMS OTPs sent to incorrect phone numbers will incur applicable Credits.
 - ii. The phone number provided by Customer must be able to receive SMS text messages. SMS OTPs sent to phone numbers unable to receive SMS text messages will incur applicable Credits.
 - iii. Customer warrants that it has obtained Users consent to receive SMS text messages.
-

OneSpan Sign

OneSpan Sign is a software platform for creating and managing the execution of digital transactions with electronic signing and delivery of Documents. Several features and options are available through OneSpan Sign. Refer to the Documentation available for review on OneSpan's Community Portal at <https://community.onespan.com> for more details. Other, optional functionalities that Customer may choose to add-on to existing product capacities ("**Components**") are available for purchase as detailed in this Service Description.

1. Definitions

"Completed Transactions" means any Transaction listed as "Completed" or "Archived" on the OneSpan Sign application dashboard.

"Document" means a single file representing a form, document or other record, not to exceed 10 megabytes of Data (the "**Document Limit**"), and capable of being viewed, electronically signed, sent or received or stored through the Service. Any Documents in excess of the Document Limit will create one or more additional new Documents

"Incomplete Transaction" means any Transaction that is not listed as a Completed Transaction on the OneSpan Sign application dashboard.

"Named User" means Customer's employee or agent who has been given login access credentials to the Account by the Administrator for purpose of accessing the Service. A Named User must be identified by a unique email address and user name, and two or more persons may not use the OneSpan Sign Service as the same Named User. **"Recorded Session"** means a recording of the Virtual Room Session with audio/visual experience.

"Session Participant" is any person joining a Virtual Room Session, including but not limited to signers and hosts..

"Session Participant Unit ("SPU") is equivalent to thirty (30) minutes per Session Participant in an active

Virtual Room Session.

“**Transaction**” means a container or package created or sent by a User associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the “**Transaction Limit**”) created or sent through the Service (includes both Incomplete and Complete Transactions). Any Documents in excess of the Transaction Limit will create one or more additional new Transactions.

“**Virtual Room Session**” is defined as a period of User activity within the Virtual Room.

2. OneSpan Sign Product Information

OneSpan Sign includes the following (as further defined in the OneSpan Sign Documentation) as part of the subscription fee:

- Web-based e-signing process that provides options for the presentation and review of Documents, methods of signature capture and user authentication, data capture and form fields.
- Workflows, reminders and notifications, attachments and e-delivery of the Documents to Users.
- Transaction management features for preparing and sending documents manually through the user interface or using transaction templates, and the ability to monitor and manage documents that are in progress or completed.
- Electronically signed Documents in PDF format with each e-signature digitally signed for comprehensive security and detection of any Document changes along with an embedded audit trail.
- An Evidence Summary Report is provided and both the electronic evidence and summary are protected by digital signing.
- A REST API along with Java and .Net SDKs to allow integrating third-party and custom applications with the Service.
- Support for native mobile applications and pre-built connectors to applications such as Salesforce and Microsoft Dynamics.

OneSpan Sign provides customers with two different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier’s discretion.

Production:

- Production usage of the current version of OneSpan Sign;
- Documents are not watermarked;
- Subject to the Service Levels.

Sandbox (Staging):

- Integration, development and testing of the current version of OneSpan Sign;
- Documents are watermarked to make them unsuitable for production usage;
Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Sandbox environment.

3. OneSpan Sign Pricing:

Confidential

Page 14 of 31

Version: May 2022

(a) Enterprise:

- OneSpan Sign Enterprise is priced based upon the number of annual Transactions or Documents committed in the applicable Order Document (“**Annual Commitment**”). Customer may exceed the Annual Commitment, but then must pay for Transactions or Documents in excess of the Annual Commitment.
- Enterprise Storage Limits:
 - a. Incomplete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction creation date, after which time Incomplete Transactions retained on the System will be charged overage charges per month of retention per Transaction (the “**Storage Fee**”); and
 - b. Complete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction completion date, after which time Complete Transactions retained on the System will be charged the Storage Fee

(b) Professional:

1. OneSpan Sign Professional is priced based on the number of individual Named Users set forth on the applicable Order Document. Professional Plans are limited to one thousand (1,000) Transactions per Named User per annual term, usage in excess of which will result in an additional Named User license fee.
2. Professional Storage Limits:
 - Incomplete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction creation date, after which time Incomplete Transactions will be deleted by Supplier; and
 - Complete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction completion date, after which time Complete Transactions retained on the System will be charged a Storage Fee.

(c) OneSpan Sign Virtual Room (“**Virtual Room**”): combines teleconference capacities, co-browsing and video/audio capabilities to provide a solution that can be accessed by the Transaction owner and signers in order proceed to an electronic agreement remotely using a “Virtual Room”. Supplier recommends Virtual Room Users maintain Internet speed of 3 Mbps or higher for optimal Product performance.

- i. Virtual Room is priced based on the number of annual Session Participant Units committed in the applicable Order Document (the “**Virtual Room Annual Commitment**”). Customer may exceed the Virtual Room Annual Commitment, but then must pay for Session Participant Units in excess of the Virtual Room Annual Commitment.
- ii. Customer must download a Recorded Session within seven (7) days of the date the recording is available for download, after which time Supplier will delete the Recorded Session.
- iii. Customer receives 400 free Sandbox (Staging) Session Participant Units (SPU) per year. Use in excess of this limit will be charged Session Participant Units.
- iv. A OneSpan Sign subscription is required for Virtual Room.

(a) Communication Hubb (for use with OneSpan Sign): see [Communication Hubb Service Description](#).

(b) OneSpan Identity Verification (for use with OneSpan Sign): see [OneSpan Identity Verification Service Description](#).

4. **OneSpan Sign General Terms:**

- Non-prepaid fees such as fees for excess usage and excess storage are invoiced quarterly in arrears; however, Supplier may elect to aggregate these fees over more than one quarter prior to invoicing for administrative convenience.
 - A Maximum of 100 signatories per Transaction are allowed, signatories in excess of this amount create an additional Transaction.
 - Unused annual Transactions, Documents, Session Participant Units and participant counts may not be carried over to the next annual term.
5. **OneSpan Sign Hold Your Own Key:** OneSpan Sign Enterprise Customers may participate in the Hold Your Own Key program subject to the Contract and the following terms:
- a. **“Hold Your Own Key” or “HYOK”** allows the Customer to use a Private Customer Master Key with the Service. **“Private Customer Master Key”** means an encryption key unique to the Customer provided by Supplier to encrypt data stored at rest. Supplier has no access to Private Customer Master Keys without Customer’s permission.
 - b. Pricing for Hold Your Own Key is on per configured self-managed key management service (“KMS”) basis. For example, if Customer has twenty accounts, ten of which are in the US, and ten of which are in Canada, but they all point to the same HYOK KMS, then only one (1) HYOK fee is charged. However, if the same Customer has the US accounts pointing to one HYOK KMS and the Canadian accounts pointing to another, then the Customer will be charged two (2) HYOK fees.
 - c. At Customer’s option, and not automatically included in the Service, Customer may elect to use a Private Customer Master Key for encryption of data at rest in OneSpan’s database which can consist of Documents, recorded evidence of the signing process, form fields entered by signers, passwords (hashed), signer authentication information, and ancillary documents. One (1) Private Customer Master Key is provided to Customer free of charge for Customers that purchase more than 100,000 Transactions annually. Customer must pay a fee for each additional key used annually. Customer may set up sub Accounts using the same Private Customer Master Key without additional charge. Customers that purchase less than 100,000 Transactions annually must pay a fee for each key used annually. Private Customer Master Key is not available for Professional Plans.
 - d. As a condition of the HYOK program, Customer agrees that notwithstanding anything to the contrary in the Contract:
 - i. CUSTOMER IS LIABLE TO AND SHALL NOT SEEK RECOVERY FROM SUPPLIER FOR ANY AND ALL CLAIMS, ACTIONS OR PROCEEDINGS (INCLUDING MISSED SERVICE LEVEL COMMITMENTS) BASED ON OR OTHERWISE ARISING OUT OF OR IN CONNECTION WITH PRIVATE CUSTOMER MASTER KEYS UNDER THE HOLD YOUR OWN KEY PROGRAM, WITHOUT LIMITATION.
 - ii. Customer agrees to indemnify and defend Supplier and its Affiliates, and their respective officers, directors, employees and agents from and against any claim, suit, proceeding, or action and pay any liabilities, damages and costs, including reasonable attorney’s fees, arising out of or in connection with Customer’s provision and use of Private Customer Master Keys.
-

EXHIBIT C: ONESPAN SAAS SERVICE LEVEL AVAILABILITY

1. Availability

Except for Maintenance Windows or as otherwise permitted herein, the SaaS Service will be available continuously at least 99.9% of the time on a monthly basis (“**Availability**”). The SaaS Service is considered unavailable when the SaaS Service is not accessible through the Internet at the point the data center connects to the public Internet for a reason other than a Force Majeure for a period of at least five (5) minutes.

General availability will be calculated per calendar month, as follows:

$$\frac{(\text{Total} - \text{Unplanned Downtime} - \text{Maintenance Window}) * 100}{\text{Total} - \text{Maintenance Window}}$$

Where:

- a. “**Total**” means the total number of minutes for the month.
- b. “**Unplanned Downtime**” occurs when the SaaS Service is unavailable for an unscheduled period of time lasting more than 5 minutes .
- c. “**Maintenance Window**” means a window in which the SaaS Service may be unavailable due to scheduled maintenance: Saturday or Sunday, from 12:00 am (midnight) to 6:00 am in the relevant time zone of the applicable data center, and up to an additional ninety (90) minutes per month of emergency maintenance at any time. Whenever reasonably possible, SaaS Service and System Maintenance is conducted in a manner so as to not impact SaaS Service availability.

2. Unavailability

For any partial calendar month within the Term, general availability will be calculated based on the entire calendar month. Should Supplier fail to achieve such Availability during any calendar month, Customer may receive a credit for the SaaS Service Fees paid for said month for each day or fraction thereof when the SaaS Service is not Available to Customer equivalent to 1/30th of the applicable monthly SaaS Service Fee, provided Customer properly requests such credit. The credit granted shall be Customer’s sole and exclusive remedy and Supplier’s sole and exclusive liability for any unavailability or downtime of the SaaS Service. In no circumstance shall the unavailability of the Subscription SaaS Services be deemed a default under the Agreement.

Customer must submit a request for credit for the SaaS Service unavailability by sending an email to support@onespan.com stating the following: (i) billing information, including company name and billing address, billing contact and billing contact phone number; and (ii) dates and time periods for each instance of downtime that Customer experienced in the relevant calendar month. Credit may only be made on a calendar month basis, and only when Customer makes the credit request within ten (10) days of the end of the calendar month when unavailability is experienced. All credit requests will be verified against Supplier’s system records. Should any credit request be disputed, Supplier will provide Customer a record of SaaS Service availability for the period in question. Any credit owed will be applied against Customer’s current or future invoices and is not refundable.

EXHIBIT D: SaaS CX PACKAGES SCHEDULE

1. Definitions

"24x5" means Monday 8 AM SGT (Singapore Time) until Friday 9 PM EST (Eastern Time) on Business Days.

"Business Days" means any day from Monday through Friday, except January 1 and December 25.

"Business Hours" means the Business Day hours listed at www.onespan.com/support based upon the Customers' geographic region corresponding to the OneSpan office providing the Support Service.

"Case" means a request for Support Services, classified by Supplier as an Incident, Support Service Request or Request for Information.

"Customer Success Manager" or **"CSM"** means the key point of contact that manages the Customer relationship. The CSM assists the Customer with its needs, desired business outcomes and manages the solution guidance required to realize value for the Customer.

"Customer Support Portal" or **"CSP"** means the web portal available at <https://support.onespan.com> where Customer may access information regarding Supplier's Support Services.

"Designated Support Specialist" means a named Supplier support agent(s) assigned to provide the Support Service.

"Engagement Manager" manages and pro-actively steers the Solution Guidance Services.

"Incident" means a request for any problem or failure that materially decreases the functionality or performance of the SaaS Service and is caused by the software, systems, networks, other components, facilities or services that are supplied as part of the SaaS Service. Incidents do not include any problem or failure caused by the use or improper use or operation of software, systems, networks, other components, facilities or services that are not part of the SaaS Service but are used to connect to, integrate with or otherwise make use of the SaaS Service.

"Onboarding Life-Cycle" means the complete lifecycle to provide Solution Guidance Services to introduce and train the Customer on the use of and integration with the SaaS Service(s) and guidance in support of the Customer's efforts to implement, test and go-live with that integrated SaaS Service(s).

"Priority Case Routing" means Case is prioritized based on CX Package tier purchased.

"Request for Information" means request for answers to questions.

"Resolution" means i) for Incidents, the correction of an error including a fix or reasonable workaround; ii) for Service Requests, the execution of the request; and iii) for Requests for Information the provision of that information.

"Response Time" means the time it takes Supplier to respond to Customer's initial request for Support Services based upon Supplier's reasonable interpretation and classification of the request. Suppliers initial response may

Confidential

[OneSpan.com](http://www.onespan.com)

Page 19 of 31

Version: May 2022

include, amongst other things, classifying the Case, confirming the Case priority and type, requesting clarification for the Case, and explaining the next steps to commencing work on Resolution.

“Service Level Objective” or “SLO” means the Response Time Support Service standards set forth in Table 2.2 as they apply to Enterprise Essential and Enterprise Elite Support Service plans for production environment Incidents only.

“Subscription Term” means the subscription term applicable to CX Package which begins on the Start Date and ends on the End Date (both as defined in the Master Terms).

“Support Service Request” means request for a change in configuration, branding, account settings, or to reset passwords, and other similar non-urgent, requests.

“Solution Architect” provides architectural leadership in the implementation of solutions through discovery, requirements gathering and workshops with customers.

“Solution Guidance Service” means consultancy services intended to (i) assist the Customer with the successful integration of the SaaS Service, (ii) provide Customer with best practices advice during the Subscription Term, and (iii) aid in the ongoing successful use of the SaaS Service.

“CX Package” is a combination of Support Services and Solution Guidance Services bundled into a package subscription service offering. There are three CX Package subscription tiers: Core, Enterprise Essential, and Enterprise Elite. CX Package options available for each tier are detailed in Tables 1, 2.1 and 2.2.

“Support Service Review” means a recurring meeting engaging Customer business and technical stakeholders and the Supplier Support Service specialist(s) to review SaaS Service and Support Service performance, with the aim to identify areas of improvement in the collaboration and track progress of such improvements.

“Support Service” means remote assistance in post-sales trouble-shooting of SaaS Service subscriptions as indicated herein

“Trust Center” means the sole platform used by Supplier to communicate upcoming releases, planned maintenance, emergency maintenance, warnings and outages for SaaS Products available for review at <https://support.onespan.com>.

2. CX Package Services

2.1 Service Hours:

The Service Hours for each CX Package are as follows:

2.1.1 **Support Service:** Support Service availability depends on the priority of the Case and the CX Package tier purchased by Customer.

2.1.2 **Solution Guidance Service:** Solution Guidance Services are provided during the Business Hours of the Supplier office providing the service and are provide up to the maximum annual Solution Guidance Service hours indicated in Table 1. Additional hours can be purchased separately at the Professional Services rates as of the date the additional hours are purchased.

2.2 **Requesting Support Services:** The Administrator may contact support via telephone and e-mail through the Customer Support Portal.

P1 and P2 Incidents must be logged by telephone. Customer must check the Trust Center to determine whether there is scheduled downtime prior to contacting Supplier.

All Cases must include a reasonably detailed written description of the decrease in functionality or performance and impact of the SaaS Service. Any Supplier time spent in the Resolution of a Case that is ultimately determined by Supplier, after

Confidential

[OneSpan.com](https://support.onespan.com)

Page 20 of 31

Version: May 2022

using commercially reasonable efforts, not to be a Supplier side defect, shall be reimbursed by the Customer on a time and materials basis.

- 2.3 **Personnel and Communication:** Supplier and the Customer will provide the necessary and appropriate personnel as required to find a Resolution. Supplier and Customer will cooperate to obtain or supply information and data, and run tests in order to assist in finding a Resolution in a timely manner.
- 2.4 **Incidents.** Supplier will use commercially reasonable efforts to deliver Incident Support Services pursuant to Tables 2.1 and 2.2.
- 2.5 **Support Service Level Objectives:** If Supplier fails to meet the Service Level Objectives, Supplier will assemble a multi-disciplinary team to work with Customer until Resolution is achieved, which is Customer's exclusive remedy and Supplier's exclusive liability for missed Service Level Objectives.
- 2.6 **Solution Guidance Services:**
 - 2.6.1 The following Solution Guidance Services are available to the Customer remotely and may include preparation, coordination, and execution of working sessions with the Customer to assist with:
 - 2.6.1.1 Onboarding and Competency Development - solution introductions, implementation and communication planning, and competency development to provide instructions on the use of the SaaS Service covering topics such as functionality descriptions, configuration parameter explanation and selection, cloud platform connectivity and security, solution administrator, API integration, and best practices.
 - 2.6.1.2 Analysis and Design – Customer requirements analysis, walkthroughs of prescribed solution workflows, and design of customer specific workflows.
 - 2.6.1.3 Implementation and Testing – Ongoing engineering guidance to assist the Customer with SaaS Service integration and testing in preparation for go live into Production.
 - 2.6.1.4 Ongoing Solution Guidance - Ongoing solution guidance, business, or architecture consultancy or competency development on the configuration, or integration of the SaaS Service.
 - 2.6.2 Only one (1) SaaS Service Onboarding Lifecycle per year is included in Solution Guidance Services; however, a single Onboarding Lifecycle may include multiple SaaS Services during the same Onboarding Lifecycle. For illustration purposes, Customer may purchase OneSpan Notary and OneSpan Sign under the same Order Document and they will both be onboarded during the same Onboarding Lifecycle (subject to the maximum annual Solution Guidance Service hours). However, if Customer purchases a SaaS Service and it is onboarded during an Onboarding Lifecycle, then later other Customer departments want to use the existing solution, the Customer must purchase additional onboarding hours separately if new-onboarding guidance is requested.
 - 2.6.3 Integration for the SaaS Service Onboarding Lifecycle is limited to one (1) electronic signature workflow for OneSpan Sign and/or one (1) electronic notary workflow for OneSpan Notary to begin using the SaaS Service in Production.
- 2.7 **Ongoing Solution Optimization**
 - 2.7.1 **Support Service Reviews.** Supplier may coordinate and conduct monthly Recurring Service Reviews with the Customer to track service performance and identify continuous performance improvements to assist with meeting Customer's evolving requirements.
 - 2.7.2 **Executive Business Reviews.** Supplier may prepare, coordinate, and conduct business review meetings at the executive level with the Customer as identified in Table 1 to review the Customer's account strategy, metrics and performance over time, evolving requirements, level of satisfaction, industry benchmarks and best practices, and any potential changes in the integrated platform.
 - 2.7.3 **Early Access to Product Releases.** Supplier may provide early access to product releases for Customers who have purchased the Enterprise Elite subscription service.
 - 2.7.4 **Release Alignment Updates.** Supplier may prepare, coordinate, and conduct release alignment meetings with the Customer to identify solution updates associated with each new product release of the SaaS Service. Supplier shall provide engineering guidance to the Customer to update their solution based on the updates associated with the latest product release as applicable to the SaaS Service. Supplier will provide early access to product releases to Customers who have purchased the Enterprise Elite subscription service.
 - 2.7.5 **Architecture and Strategy Workshops.** Supplier may prepare, coordinate, and conduct periodic workshops with Customers who have purchased the Enterprise Elite subscription service to review evolving Customer architecture requirements and make recommendations on how best to adjust their integrated solution accordingly.
 - 2.7.6 **Health Checks.** Supplier may prepare, coordinate, and conduct periodic health checks of the Customer's integrated solution and make recommendations on how to improve any performance inconsistencies.

Confidential

[OneSpan.com](https://www.one-span.com)

Page 21 of 31

Version: May 2022



- 2.7.7 **Use Case Validation.** Supplier may prepare, coordinate, and conduct periodic workshops with Customers who have purchased the Enterprise Elite subscription service to review required use cases and provide guidance on how to implement them within the solution purchased.
- 2.7.8 **Best Practices Workshops.** Supplier may host a best practices workshop geared toward providing Customer with advice on implementing an efficient and scalable solution and optimizing time to value and facilitating adoption.

Table 1 – CX Packages

Description	Core	Enterprise Essential	Enterprise Elite
SaaS P1 & P2 Incident Support (24 x 7)	Trust Center	Telephone	Telephone
Support Case Channel (*)	CSP / Email	Telephone CSP / E-mail	Telephone CSP / E-mail
Knowledgebase & Developer Community	✓	✓	✓
Root cause analysis for P1 Incidents upon request		✓	✓
Service Level Objectives		✓	✓
Support Service Review Upon Request		1 per quarter	1 per month
Executive Business Review Upon Request		1 per year	2 per year
Release Alignment Update		✓	✓
Priority Case Routing		✓	✓
Escalation Management		✓	✓
Solution Guidance Service		✓	✓
Use Case Validation		✓	✓
Best Practices Workshops		✓	✓
Maximum Annual Solution Guidance Service Hours		112 hours	160 hours
Continuous New Release Alignment		At most 4 per year	At most 4 per year
Customer Success Manager		Shared	Named
Engagement Manager		Shared	Named
Solution Architect			Named
Designated Support Specialist			Named
Cadence calls intended to expedite Case Resolution as agreed with Customer (Support Status review meeting)			✓
Dedicated Hotline			✓
Architecture and Strategy Workshops			✓

Confidential

OneSpan.com

Page 23 of 31

Version: May 2022

Early Access to Product Releases	✓
Health Checks	✓

(*) As per the Service Levels as defined in Tables 2.1 and 2.2 – Case Type Classification and Response Times Per Channel.

Table 2.1 – Core Success – Case Classification and Response Times

Case		Channel	Response Time
Incident	P1	E-mail and CSP Trust Center status updates (24 x 7)	8 Business hours
	P2	E-mail and CSP Trust Center status updates (24 x 7)	8 Business hours
	P3	E-mail and CSP	Next Business Day
	P4	E-mail and CSP	Commercially reasonable efforts
Service Request (P3-P4)		E-mail and CSP	Next Business Day
Request for Information (P3-P4)		E-mail and CSP	Commercially reasonable efforts

Table 2.2 – Enterprise Essential / Enterprise Elite – Case Classification and Response Times

Case		Channel	Availability	Response Time	Response Time SLO	Commencing Work	Status updates
Incident	P1	Telephone	24 x 7	5 mins	100 %	<1 hour Work continuously	Every 1 hour
		E-mail and CSP	Business Days (24x5)	1 hour			
	P2	Telephone	24 x 7	5 mins	100 %	<1 Business Hour Work continuously during 24 x 5	Every 2 hours
		E-mail and CSP	Business Days (24x5)	1 hour			
	P3	E-mail and CSP	Business Days (24x5)	4 hours	95 %	8 Business Hours	-
	P4	E-mail and CSP	Business Days (24x5)	4 hours	95 %	8 Business Hours	-
Service Request (P3-P4)		E-mail and CSP	Business Days (24x5)	8 hours	-	8 Business Hours	-
Request for Information (P3-P4)		E-mail and CSP	Business Hours (8 x 5)	8 Business Hours	-	Commercially reasonable efforts	-

Table 3 – Incident Priority Matrix

			Impact		
			Low	Medium	High
			• Affects few of Customers' Users (30 % or lower) • Affects the operations in a production or non-production environment • Customer experiencing low business impact	• Affects most of Customers' Users (>30 %) • Affects the operations in a production environment • Customer experiencing medium business impact	• Affects all Customers' Users • Affects the operations in a production environment • Customer experiencing high business impact
r g e n c y	o w	• Customer is experiencing occasional stoppage • Workaround is available • Non-business critical functionality • Examples include, but are not limited to, images missing on webpages, text errors, documentation issues	P4	P3	P2
	e d i u m	• Customer is experiencing a partial or occasional stoppage • Work-around is cumbersome to use • Business critical functionality • Examples include, but are not limited to, performance degradation, non-production issues that block project execution, Service Requests, signed document packages not available, reports missing, document triggers not working properly, web administrator issues, rule creation issues	P3	P2	P1
	i g h	• Customer is experiencing continuous stoppage • No workaround available to restore Customer to normal business operations • Business critical functionality • Examples include, but are not limited to, document signature request fails, authentication/signature verification fails, scoring requests fail	P2	P1	P1

3. Conditions and Exclusions

CX Packages do not include:

- (a) Diagnosis and rectification of any error resulting from:
 - i. use of SaaS Service after CX Packages have terminated or expired
 - ii. direct or indirect operator error or omission
 - iii. failure of the Customer to implement recommendations advised by Supplier
 - iv. use, operation, or merger of the SaaS Service with hardware, software, or programming languages or in an environment other than that for which the SaaS Services are designed or authorized by Supplier
 - v. a bug, error, defect in, or failure of any software operating in conjunction with the SaaS Service not supplied or authorized by Supplier
- (b) Order status follow-up
- (c) Enhancements
- (a) Installation, configuration, backup or management of any third party software or hardware (such as operating systems, databases, network settings, backup systems, monitoring solution, Active Directory or other Windows Services, load balancers, server hardware, firewall.)
- (b) Custom documentation, development and training materials
- (c) Solution Guidance Services outside Service Hours. (Available at an additional expense through a separate agreement at the Professional Services rates as of the date the additional hours are purchased.)
- (d) Solution guidance services can be provided on-site at Customer's location subject to an additional travel and lodging expense billed separately.
- (e) More than one (1) SaaS Service Onboarding Lifecycle per year. Solution Guidance Services for additional SaaS Service Onboarding Lifecycles are available in a separate agreement at the Professional Services rates as of the date the additional hours are purchased.
- (f) More than the minimum number of workflows necessary to begin using the SaaS Service in Production. Solution Guidance Services for the integration of additional workflows are available in a separate agreement at the Professional Services rates as of the date the additional hours are purchased.

If Customer requires assistance or service not covered by CX Packages, Customer may contact a Supplier representative to obtain the applicable Service at an additional cost.

4. Customer's Responsibilities

For the delivery of Support Services, the Customer must:

- (a) ensure sufficient access to the Internet for remote screen share when deemed necessary for expedited Resolution
- (b) ensure that the latest version of the SaaS Service is in use for optimal Support Service
- (c) ensure that Customer Designated Contact(s) (i) are up-to-date in their knowledge of the SaaS Service in its latest version; (ii) have access to all data relevant to the SaaS Service; (iii) provide Supplier with all information for proper issue diagnosis and troubleshooting, including information on the relevant environment (e.g. additional log-files) to reproduce the issue; and (iv) provide timely replies
- (d) not transfer to Supplier any Customer's client-related information unless anonymized
- (e) allow Supplier to carry out Support Service outside of Customer's normal working hours as may be necessary
- (f) give timely written notice to Supplier of any change in the Customer Administrators

Failure of Customer to meet its responsibilities or provide sufficient information may heavily delay or render impossible the provisioning of Support Service.

5. Pricing; Term and Termination

5.1 CX Package.

Confidential

[OneSpan.com](https://www.onespan.com)

Page 27 of 31

Version: May 2022

(a) Core. Core CX Packages are included in, are conterminous with and renew with the SaaS Service subscription. Customer may upgrade to Enterprise Essential or Enterprise Elite at any time during a term; however, Customer may not downgrade until the next renewal period.

(b) Enterprise Essential and Enterprise Elite. Enterprise Essential and Enterprise Elite CX Packages are charged at the rates indicated in the applicable Order Document. Enterprise Elite CX Packages are coterminous with and renew with the SaaS Service subscriptions. Customer may upgrade Enterprise Essential CX Packages to Enterprise Elite CX Packages at any time during a term; however, Customer may not downgrade until the next renewal period.

5.2 End of Life. Unless otherwise terminated in accordance with the terms herein, CX Packages and Products will expire pursuant to the End of Life Policy made generally available to Supplier's Customers on Supplier's website at <https://www.onespan.com/support/security/product-life-cycle>.

EXHIBIT E: SERVICE USE GUIDELINES AND CONDITIONS

1. Service Use Guidelines

Customer will not, and will not permit any of its Users or deliberately enable any other third party, to:

- (a) modify, copy, display, republish or create derivative works based on the SaaS Service, the underlying software or any content;
- (b) frame, scrape, link to or mirror any content forming part of the SaaS Service;
- (c) reverse engineer, decompile, decrypt or attempt to discover any source code or underlying ideas or algorithms of the SaaS Service or the underlying software and components;
- (d) disclose the results of any benchmark testing, technical results or other performance data relating to use of the SaaS Service or the underlying software and components;
- (e) access the SaaS Service or allow others to access the SaaS Service in order to: (a) build a competitive product or service, (b) build a product using similar ideas, features, functions or graphics of the SaaS Service, or (c) copy any ideas, features, functions or graphics of the SaaS Service;
- (f) use the SaaS Service in connection with any illegal, defamatory, harassing, libelous, threatening, or obscene material or purpose or to send any message or material that in any way violates or infringes upon the intellectual property rights or the privacy or publicity rights of any person or entity or that may otherwise be unlawful or give rise to civil or criminal liability;
- (g) send or allow any Malicious Code through the SaaS Service and/or System;
- (h) copy, publish or reproduce the SaaS Service and/or System for others to copy or use any component thereof except as expressly permitted herein;
- (i) distribute, re-distribute, sublicense, assign, share, sell, resell, time-share, rent, lease or otherwise make the SaaS Service available to any third party (except as expressly contemplated in this Contract), or grant a security interest in the SaaS Service;
- (j) interfere or attempt to interfere in any manner with the functionality or proper working of the SaaS Service and/or System, or disrupt the integrity or performance of the SaaS Service and/or System or any data contained therein;
- (k) circumvent any contractual, technical or logical use, Customer or User restrictions agreed upon or existing in the SaaS Service and/or System or attempt to gain unauthorized access to, or use of, any part of the SaaS Service and/or System; or
- (l) perform any form of stress, load, performance, security or other vulnerability or penetration tests on the SaaS Service and/or System.

2. Service Conditions

Use of the SaaS Service by Customer, its Users is subject to the following conditions:

- (a) Customer maintains control of or access to Data and sole control over the content, quality, and format of any Data provided;
- (b) Customer is solely responsible for ensuring that Customer's use of the SaaS Service complies with all applicable laws, including any electronic signature, audio and video recording, consumer, data protection, data privacy and trade control laws;
- (c) Customer may elect to deploy third party features within the SaaS Service designed to verify the identity of the Users ("Identity Verification Measures"). Supplier: (i) will apply only those Identity Verification Measures (if any) selected by Customer, (ii) makes no representations or warranties regarding the appropriateness of such Identity Verification Measures and whether Users have the necessary knowledge or ability to successfully meet such Identity Verification Measures, and (iii) assumes no liability or responsibility for the circumvention by any User or other person of any Identity Verification Measures. Customer shall comply with the applicable Identity Verification Measures Terms which

Confidential

OneSpan.com

Page 29 of 31

Version: May 2022



are incorporated into this Schedule by reference and are available for review at <https://www.onespan.com/third-party-terms>;

- (d) for Customer initiated email and SMS communications through the SaaS Service, Customer shall comply with, as applicable, the United States CAN-SPAM Act, Canada's Anti-Spam Law, , the E.U. Directive on Privacy and Electronic Communications, Do-Not-Call Implementation Act or any other applicable anti-Spam, do not call, or similar laws. Customer is solely responsible to obtain User consent to receive promotional or marketing content via email or SMS through the SaaS Service, and to provide its Users with the ability to opt-out of e-mail and SMS communications generated through the SaaS Service and Customer shall comply with its Users communication preferences;
- (e) Customer warrants that neither it nor its customer will send SMS content that is illegal, unauthorized, prohibited, fraudulent, deceptive, inaccurate, or misleading (including, without limitation, by using a false identity or forged address or telephone number), and will not send SMS content in violation of any applicable law or would otherwise cause Supplier or its licensors to be in violation of applicable law, Customer bears sole and exclusive responsibility for its Users' use of the SaaS Service.
- (f) Customer shall refer to the SaaS Service by its URL, as required, and not reply upon Supplier's IP address. Supplier expressly reserves the right to alter its IP addressing at any time with no prior notification to Customer or any other party, including but not limited for purposes of disaster recovery data or center relocation;
- (g) Supplier does not monitor content processed through the SaaS Service, but it may suspend any use of the SaaS Service, if Supplier reasonably and in good faith believes Customer use violates the terms of this Contract or applicable laws or regulations. Supplier will use commercially reasonable efforts to notify Customer prior to any such suspension or disablement, unless Supplier: (i) is prohibited from doing so under applicable law, court order or under legal process; or (ii) deems it necessary to delay notice in order to prevent imminent harm to the SaaS Service, or a third party;
- (h) Supplier may modify the SaaS Service from time to time, in its discretion, without notice to the Customer, for the purpose of improving SaaS Service features, functions or performance, provided that no such modification shall materially reduce the level or quality of the SaaS Service, as offered as of the Effective Date. Notwithstanding the foregoing, Supplier may apply any improvements and modifications to the SaaS Service and/or System required to maintain Supplier's legal and regulatory requirements, as well as security standards including, but not limited to, any security standards listed in the Privacy and Security terms. It is Customer's sole responsibility to maintain the security of Customer's computer systems and comply with any industry standard minimum security requirements to gain access to the SaaS Service;
- (i) Except for Data and the limited Personal Data that may be provided by Customer to Supplier to the extent necessary to administer the business relationship between the parties (such as for invoicing and billing purposes), Customer warrants that it shall at no time transfer or provide or otherwise make accessible any Personal Data (as defined in the Privacy and Security terms) to Supplier, including, without limitation, for the purpose of receiving any support and maintenance services;
- (j) Supplier shall not be obligated to provide any Data to any Users or third parties. Customer acknowledges that it is solely responsible for the management of its own record and data retention record policy, including for determining how long any Data and other records are required to be retained or stored under any applicable laws, regulations, or legal or administrative agency processes;
- (k) Customer is solely responsible for obtaining and maintaining, and for assuring that its Users obtain and maintain any hardware and software, for contracting with an Internet service provider, a telecommunications carrier or other service provider for services necessary to establish Customer's and User's connection or access to the Internet and the SaaS Service;
- (l) To maintain reliability and stability of the SaaS Service, Supplier continually monitors the load being imposed on the SaaS Service by Customers using integrated applications. Supplier may request that a Customer placing an unnecessary burden on the SaaS Service take measures to reduce their load on the SaaS Service. In addition, the SaaS Service and/or System may also automatically reduce the load being accepted by the SaaS Service through internal system controls; and
- (m) Supplier may temporarily suspend Customer's access or use of any portion or all of the SaaS Service immediately if Supplier determines that (i) Customer or a Customer User's use of the SaaS Service (a) poses a security risk to the SaaS Service or any third party, (b) could adversely impact Supplier's systems, or the SaaS Service or the content of any other Supplier customer, (c) could subject Supplier, its Affiliates, or any third party to liability, or d) could be fraudulent; or (ii) that Customer's account security has been, or is reasonably expected to have been compromised. If Supplier suspends Customer's right to access or use any portion of the SaaS Service, Customer (x) will provide

reasonable assistance to Supplier in rectifying the issue(s) leading to the suspension, (y) remains responsible for all fees incurred during the period of suspension, and (z) is not entitled to any service credits during the suspension period.