

## State of Oregon

### DocuSign Services Agreement

This DocuSign Services Agreement sets forth the terms and conditions between the State of Oregon, acting by and through its Department of Administrative Services, and Carasoft Technology Corporation (“Reseller”) under which, in addition to the Reseller Agreement (as defined below), Reseller will deliver to Authorized Purchasers (as defined in the Reseller Agreement) the DocuSign Signature Services and the DocuSign CLM Services provided by DocuSign, Inc. (“DocuSign”) purchased by Authorized Purchasers under the Reseller Agreement. This agreement and the following attached documents, each of which is incorporated by reference, shall be referred to herein as the “**DocuSign Services Agreement**”:

1. the DocuSign Master Services Agreement, which is attached hereto as Attachment I, and
2. the Service Schedule for DocuSign Signature, which is attached hereto as Attachment II,
3. the Security Attachment for DocuSign Signature, which is attached hereto as Attachment III,
4. the DocuSign CLM Service Schedule, which is attached hereto as Attachment IV,
5. the Security Attachment for DocuSign CLM, which is attached hereto as Attachment V,
6. The Letter dated 4/7/2021 from the Reseller to State of Oregon, which is attached hereto as Attachment VI (the “Reseller Price Guarantee”), and

#### **A. General Terms.**

**1. Reseller Agreement.** Reseller is making the Services available to Agency under that certain Participating Addendum, State of Oregon Contract Number 9412, to the NASPO ValuePoint Cloud Solutions Master Agreement No. AR2472, entered into by and between Carasoft Technology Corp and the Oregon Department of Administrative Services, Procurement Services (the “**Reseller Agreement**”). Reseller acknowledges and agrees that the DocuSign Services Agreement shall govern the use of any DocuSign Services purchased by an Authorized Purchaser under the Reseller Agreement.

**2. Definitions.** Capitalized terms not defined in this Rider shall have the meanings assigned to them in the DocuSign Services Agreement, provided that the following terms used in the DocuSign Services Agreement will have the meaning set forth below when used therein and in this Rider.

**2.1. “Customer”** is the “Authorized Purchaser” purchasing the Services under the Reseller Agreement, as the term “Authorized Purchaser” is defined in the Reseller Agreement.

**2.2 “DocuSign Services”** means “Cloud Solutions” and “Related Services” as defined in the Reseller Agreement.

**3. Carahsoft as Reseller.** Reseller represents and warrants that:

**3.1** It is authorized to sell to Agency the DocuSign Services pursuant to the Reseller Agreement and this DocuSign Services Agreement;

**3.2** It has the authority to both bind DocuSign to the terms of this DocuSign Services Agreement and will, at all times during the Term, cause DocuSign to comply with the provisions set forth in Exhibit B to the Reseller Agreement; and

**3.3** DocuSign will provide the Services specified in this DocuSign Services Agreement in compliance the Reseller Agreement, including its Exhibits B and each of the Attachments to this DocuSign Services Agreement.

**4. Reseller Indemnity.** Reseller shall defend and indemnify and hold Authorized Purchasers, the State of Oregon, and their respective agents, officials, officers, directors, and employees harmless from all third party claims, demands, suits, actions, proceedings, losses, liabilities, settlements, damages, awards, and costs (including reasonable attorneys' fees and expenses at trial, on appeal and in connection with any petition for review), which may be brought or made against any Authorized Purchaser, the State of Oregon, or their respective agents, officials, officers, directors, or employees (i) arising out of or related any damages or liability incurred by Authorized Purchaser based on an act or omission of DocuSign in violation of DocuSign's obligations under the DocuSign Services Agreement, or (ii) by DocuSign based on any act or omission of the Authorized Purchaser that is permitted under the DocuSign Services Agreement.

**5. Scope of Rider; Services; Price Guarantee.**

**5.1. Scope of DocuSign Services Agreement.** This DocuSign Services Agreement is limited to the purchase of any DocuSign Services under the Reseller Agreement by an Authorized Purchaser.

**5.2 Service Descriptions.** During the Term of the Reseller Agreement, Reseller shall provide the DocuSign Services to Authorized Purchasers who purchase DocuSign Services under the Reseller Agreement as agreed to in this DocuSign Services Agreement.

**5.3 Price Guarantee.** Reseller will provide quotes to Authorize Purchasers for the DocuSign Services and will charge Authorized Purchasers for the DocuSign Services in accordance with the terms of the Reseller Price Guarantee and the DocuSign Price Guarantee.

**6. Order of Precedence.** In the event of any conflict between the Reseller Agreement, this Rider, and Attachments I-V, the conflict shall be resolved in the following descending order:

- The Reseller Agreement, including each of its exhibits, attachments and schedules
- This DocuSign Services Agreement, less its Attachments
- The DocuSign Master Services Agreement
- The applicable Service Schedule for the DocuSign Services (i.e., Attachment II or IV to this


Rider)

- The applicable Security Attachment for the DocuSign Services (i.e., Attachment III or V to this Rider).

[Signatures to follow]

**RESELLER, BY EXECUTION OF THIS AGREEMENT, HEREBY ACKNOWLEDGES THAT IT HAS READ THIS DOCUSIGN SERVICES AGREEMENT , UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS.**

**Carahsoft Technology Corporation**

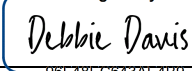
By:   
FF1FF4951BF0483

Name: Bethany Blackwell

Title: Vice President

Date: 4/15/2021

**The State of Oregon, acting by and through its Department of Administrative Services, Procurement Services:**

By:   
96F48EC643AE4B9...

Name: Debbie Davis

Title: State Procurement Analyst

Date: 4/15/2021

**The State of Oregon, Department of Justice**

By: John McCormick via email dated 4/13/2021

Title: Assistant Attorney General

## ATTACHMENT I

### DOCUSIGN MASTER SERVICES AGREEMENT

This DocuSign Master Services Agreement (“MSA”) is made between DocuSign, Inc., a Delaware corporation, (“DocuSign”) and the State of Oregon, acting through its Department of Administrative Services, Purchasing Services (DAS PS). The purpose of this MSA is to establish the terms and conditions of individual contracts entered into by Authorized Purchasers (as defined in the Reseller Agreement) that issue purchase orders under the Reseller Agreement to establish individual contracts to acquire DocuSign Services under the Reseller Agreement. DAS PS is not party to any contract entered into by an Authorized Purchaser unless DAS PS is the entity submitting the purchaser order under the Reseller Agreement that is the basis for any such contract.

Each Authorized Purchaser that enters into an Agreement (as defined below) for DocuSign Services under the Reseller Agreement will be referred to herein as the “Customer” and, together with DocuSign, shall be referred to herein as the “Parties” and each of DocuSign and the Customer individually as a “Party.” Each Agreement entered into hereunder will also include specific services terms, product details and any applicable license and/or subscription terms, which will be set forth in applicable [Service Schedule\(s\)](#) attached to this MSA, Order Form(s) and SOW(s), each of which become binding on the Parties to each Agreement and incorporated into such Agreement upon execution of an Order Form and/or SOW that incorporates those Service Schedules. Each agreement established by an Order Form or SOW (or both) is governed by and incorporates the following documents, collectively referred to as the “Agreement” that consists of:

1. the Order Form and any Statement of Work included with it;
2. any attachments and/or appendix(ices) to a Service Schedule;
3. Service Schedule(s); and
4. this MSA.

The applicable attachment(s), appendix(ices), and Service Schedule(s) is determined by the DocuSign Service(s) purchased on the Order Form and/or SOW. In the event of a conflict, the order of precedence is as set out above in descending order of control.

Each Agreement entered into under this MSA is a separate and distinct contract between DocuSign and the Authorized Purchaser (as defined in the Reseller Agreement) submitting the Order Form, separate and distinct from each other Agreement entered into under this MSA.

MSA Version: December 18, 2019.

Each Party agrees that the following terms and conditions govern each Agreement entered into under -this MSA:

#### TABLE OF CONTENTS

1. [Definitions](#)
2. [Usage and Access Rights](#)
3. [Ownership](#)

4. [Security and Customer Data](#)
5. [Payment of Fees](#)
6. [Taxes](#)
7. [Term and Termination](#)
8. [Warranties and Disclaimers](#)
9. [Third-Party Claims](#)
10. [Limitation of Liability](#)
11. [Confidentiality](#)
12. [Governing Law and Venue](#)
13. [General](#)

## 1. DEFINITIONS

“Account” means a unique account established by Customer to enable its Authorized Users to access and use a DocuSign Service.

“Account Administrator” is an Authorized User who is assigned and expressly authorized by Customer as its agent to manage Customer’s Account, including, without limitation, to configure administration settings, assign access and use authorizations, request different or additional services, provide usage and performance reports, manage templates, execute approved campaigns and events, assist in third-party product integrations, and to receive privacy disclosures. Customer may appoint an employee or a third-party business partner or contractor to act as its Account Administrator and may change its designation at any time through its Account.

“Affiliate” of a Party means (i) with respect to DocuSign, any entity that DocuSign directly or indirectly owns or controls more than fifty percent (50%) of the voting interests of the subject entity, and any legal entity will be considered DocuSign’s Affiliate as long as that interest is maintained, and (ii) with respect to Customer, any Public Body (as defined at ORS 174.109) to which Customer provides services that require use of the DocuSign Services.

“Authorized User” means one individual natural person, whether an employee, business partner, contractor, or agent of Customer or its Affiliates who is registered by Customer to use the DocuSign Services. An Authorized User must be identified by a unique email address and user name, and two or more persons may not use the DocuSign Services as the same Authorized User. If the Authorized User is not an employee of Customer, use of the DocuSign Services will be allowed only if the user is under confidentiality obligations with Customer at least as restrictive as those in this Agreement and is accessing or using the DocuSign Services solely to support Customer’s and/or Customer Affiliates’ internal business purposes.

“Confidential Information” means (a) for DocuSign and its Affiliates, the DocuSign Services and Documentation; (b) for Customer and its Affiliates, Customer Data; and (c) any other information of a Party or its Affiliates that is disclosed in writing or orally and is designated as confidential or proprietary at the time of disclosure to the Party, including its Affiliates, receiving Confidential Information (“Recipient”) (and, in the case of oral disclosures, summarized in writing and delivered to the Recipient within thirty (30) days of the initial disclosure), or that due to the nature of the information the Recipient would clearly understand it to be confidential information of the disclosing Party. Confidential Information does not include any information that: (i) was or becomes generally known to the public through no fault or breach of this Agreement by the

Recipient; (ii) was rightfully in the Recipient's possession at the time of disclosure without restriction on use or disclosure; (iii) was independently developed by the Recipient without use of or reference to the disclosing Party's Confidential Information; or (iv) was rightfully obtained by the Recipient from a third party not under a duty of confidentiality and without restriction on use or disclosure.

"Customer Data" means any content, eDocuments, materials, data and information that Customer or its Authorized Users enter into the DocuSign Cloud Services, including, but not limited to, any Customer personal data and information contained in eDocuments. Customer Data does not include any component of the DocuSign Services or material provided by or on behalf of DocuSign.

"Documentation" means DocuSign's then-current technical and functional documentation for the DocuSign Services as made generally available by DocuSign.

"DocuSign Cloud Service(s)" means any subscription-based, hosted solution that is supported and operated on demand and provided by DocuSign under this Agreement.

"DocuSign Service(s)" means the services identified on the Order Form and/or SOW and obtained by Customer pursuant to this Agreement, including but not limited to DocuSign Cloud Services and Professional Services.

"eDocument" refers to a contract, notice, disclosure, or other record or document deposited into the DocuSign Cloud Service by Customer for processing.

"Indemnified Party(ies)" means, as the case may be, the Party (whether DocuSign or Customer) being indemnified for a third-party claim, including its employees, directors, agents, and representatives.

"Indemnifying Party(ies)" means the Party (whether DocuSign or Customer) that is providing indemnification under Section 9 (Third-Party Claims).

"Order Form" means the order form issued to the Reseller pursuant to the Reseller Agreement that sets forth the pricing and options of the DocuSign Services selected by Customer.

"Order Start Date" means the start date of the applicable Order Form as defined in that Order Form.

"Professional Services" means any integration, consulting, architecture, training, transition, configuration, administration, and similar ancillary DocuSign Services that are set forth in an Order Form or Statement of Work ("SOW").

"Reseller Agreement" means an agreement between DAS PS or another agency of the State of Oregon and an authorized reseller of DocuSign Services that sets forth the terms and conditions under which an agency of the State of Oregon, or a member of a cooperative procurement group (as defined at ORS 279A.200(1)(c)) of which the State of Oregon is a member may purchase DocuSign Services.

“Service Schedule” means the service-specific terms and conditions applicable to the DocuSign Service(s).

## 2. USAGE AND ACCESS RIGHTS

2.1 Right to Use. DocuSign will provide the DocuSign Services to Customer as set forth in the Order Form and/or SOW. Subject to the terms and conditions of this Agreement, DocuSign grants to Customer a worldwide, limited, non-exclusive, non-transferrable right and license during the Term, solely for its and its Affiliates’ internal business purposes, and in accordance with the Documentation, to: (a) use the DocuSign Services; (b) implement, configure, and through its Account Administrator, permit its Authorized Users to access and use the DocuSign Services; and (c) access and use the Documentation. Customer will ensure that its Affiliates and all Authorized Users using the DocuSign Services under its Account comply with all of Customer’s obligations under this Agreement, and Customer is responsible for their acts and omissions relating to the Agreement as though they were those of Customer.

2.2 Restrictions. Customer shall not, and shall not permit its Authorized Users or others under its control to do the following with respect to the DocuSign Services:

- (a) use the DocuSign Services, or allow access to it, in a manner that circumvents contractual usage restrictions or that exceeds Customer’s authorized use or usage metrics set forth in this Agreement, including the applicable Order Form or SOW;
- (b) license, sub-license, sell, re-sell, rent, lease, transfer, distribute, time share or otherwise make any portion of the DocuSign Services or Documentation available for access by third parties except as otherwise expressly provided in this Agreement;
- (c) access or use the DocuSign Services or Documentation for the purpose of: (i) developing or operating products or services intended to be offered to third parties in competition with the DocuSign Services, or (ii) allowing access to its Account by a direct competitor of DocuSign;
- (d) reverse engineer, decompile, disassemble, copy, or otherwise attempt to derive source code or other trade secrets from or about any of the DocuSign Services or technologies, unless and then only to the extent expressly permitted by applicable law, without consent;
- (e) use the DocuSign Services or Documentation in a way that (i) violates or infringes upon the rights of a third party, including those pertaining to: contract, intellectual property, privacy, or publicity; or (ii) effects or facilitates the storage or transmission of libelous, tortious, or otherwise unlawful material including, but not limited to, material that is harassing, threatening, or obscene;
- (f) fail to use commercially reasonable efforts to not interfere with or disrupt the integrity, operation, or performance of the DocuSign Services or interfere with the use or enjoyment of it by others;
- (g) use the DocuSign Services to create, use, send, store, or run viruses or other harmful computer code, files, scripts, agents, or other programs, or circumvent or disclose the user authentication or security of the DocuSign Cloud Service or any host, network, or account related thereto or use any

aspect of the DocuSign Services components other than those specifically identified in an Order Form or SOW, even if technically possible; or

(h) use, or allow the use of, the DocuSign Services in violation of Section 13.5 (Trade Restrictions).

**2.3 Suspension of Access.** DocuSign may suspend any use of the DocuSign Services, or remove or disable any Account or content that DocuSign reasonably and in good faith believes violates this Agreement. DocuSign will use commercially reasonable efforts to notify Customer prior to any such suspension or disablement, unless DocuSign reasonably believes that: (a) it is prohibited from doing so under applicable law or under legal process (such as court or government administrative agency processes, orders, mandates, and the like); or (b) it is necessary to delay notice in order to prevent imminent harm to the DocuSign Services or a third party. Under circumstances where notice is delayed, DocuSign will provide notice if and when the related restrictions in the previous sentence no longer apply. Notwithstanding the foregoing, DocuSign may not limit Customer's access to Customer Data stored in the DocuSign Services unless DocuSign determines that allowing such access would jeopardize the security of the DocuSign Services.

**2.4 Trial Usage.** If Customer registers for a free trial, promotional offer, or other type of limited offer for use of the DocuSign Services ("Free Trial"), Customer may be presented with additional terms and conditions when registering for a Free Trial, and any such additional terms and conditions are hereby incorporated into this Agreement by reference as a Service Schedule and are legally binding upon the Parties. ANY DATA THAT CUSTOMER ENTERS INTO THE DOCUSIGN SERVICES, AND ANY CONFIGURATIONS MADE BY OR FOR CUSTOMER, DURING THE FREE TRIAL WILL BE PERMANENTLY LOST AT THE END OF THE TRIAL PERIOD UNLESS CUSTOMER: (a) PURCHASES A SUBSCRIPTION TO THE SAME DOCUSIGN SERVICES AS THOSE COVERED BY THE TRIAL; (b) PURCHASES AN UPGRADED VERSION OF THE DOCUSIGN SERVICES; OR (c) EXPORTS SUCH DATA BEFORE THE END OF THE TRIAL PERIOD. CUSTOMER CANNOT TRANSFER DATA ENTERED OR CONFIGURATIONS MADE DURING THE FREE TRIAL TO A DOCUSIGN SERVICE THAT WOULD BE A DOWNGRADE FROM THAT COVERED BY THE TRIAL, AND IN SUCH SITUATION ANY CUSTOMER DATA OR CUSTOMIZATION WILL BE PERMANENTLY LOST. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, INCLUDING WITHOUT LIMITATION SECTION 8 (WARRANTIES AND DISCLAIMERS), SECTION 9 (THIRD-PARTY CLAIMS), AND SECTION 10 (LIMITATION OF LIABILITY), FREE TRIALS ARE PROVIDED "AS-IS" AND "AS AVAILABLE" AND, TO THE FULLEST EXTENT PERMISSIBLE BY LAW, (y) WITHOUT ANY REPRESENTATION OR WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY; AND (z) DOCUSIGN'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO CUSTOMER'S USE OF THE FREE TRIAL IS \$100.

### 3. OWNERSHIP

**3.1 Customer Data.** Customer Data processed using the DocuSign Services is and will remain, as between Customer and DocuSign, owned by Customer. Customer hereby grants DocuSign the right to process, transmit, store or disclose the Customer Data in order to provide the DocuSign Services to Customer subject to the terms of Section 11.2 (Required Disclosure) below.



3.2 **DocuSign Services.** DocuSign, its Affiliates, or its licensors own all right, title, and interest in and to any and all copyrights, trademark rights, patent rights, database rights, and other intellectual property or other rights in and to the DocuSign Services and Documentation, any improvements, design contributions, or derivative works thereto, and any knowledge or processes related thereto and/or provided hereunder. Unless otherwise specified in the applicable SOW, all deliverables provided by or for DocuSign in the performance of Professional Services, excluding Customer Data and Customer Confidential Information, are owned by DocuSign and constitute part of the DocuSign Service(s) under this Agreement.

3.3 **Third-Party Services or Materials.** Customer may choose to obtain products, services or materials that are provided or supported by third parties (“Third-Party Services and Materials”) for use with DocuSign Services. DocuSign assumes no responsibility for, and specifically disclaims any liability or obligation with respect to, any Third-Party Services and Materials that are provided pursuant to the terms of the applicable third-party license or separate agreement between the licensor of the Third-Party Services and Customer. DocuSign does not represent and/or warrant in any manner that Third-Party Services and Materials are accurate, current, or comply with laws, rules and/or regulations of, or are otherwise valid and enforceable in or appropriate for, the jurisdiction in which the Third-Party Services and Materials are used or for Customer’s purposes.

3.4 **Feedback.** DocuSign encourages Customer to provide suggestions, proposals, ideas, recommendations, or other feedback regarding improvements to DocuSign Services and related resources (“Feedback”). To the extent Customer provides Feedback, Customer grants to DocuSign a royalty-free, fully paid, sub-licensable, transferable (notwithstanding Section 13.2 (Assignability)), non-exclusive, irrevocable, perpetual, worldwide right and license to make, use, sell, offer for sale, import, and otherwise exploit Feedback (including by incorporation of such feedback into the DocuSign Services) without restriction; provided that such Feedback does not identify Customer, its Affiliates, or Authorized Users, or include any Customer Data without Customer’s prior written consent.

## 4. SECURITY AND CUSTOMER DATA

4.1 **Security.** DocuSign will use commercially reasonable industry standard security technologies in providing the DocuSign Services. DocuSign has implemented and will maintain appropriate technical and organizational measures, including information security policies and safeguards, to preserve the security, integrity, and confidentiality of Customer Data and personal data and to protect against unauthorized or unlawful disclosure or corruption of or access to personal data. Additional security obligations, if any, shall be set forth or referenced in the applicable Service Schedule, attachment and/or appendix.

4.2 **Customer Data.** Customer is responsible for Customer Data (including Customer personal data) as entered into, supplied or used by Customer and its Authorized Users in the DocuSign Services. Further, Customer is solely responsible for determining the suitability of the DocuSign Services for Customer’s business and complying with any applicable data privacy and protection regulations, laws or conventions applicable to Customer Data and Customer’s use of the DocuSign Services. Customer grants to DocuSign the non-exclusive right to process Customer Data (including personal data) in accordance with the applicable data protection provisions and the technical and organizational measures referred to in an applicable Service Schedule, attachment

and/or appendix, for the sole purpose of and only to the extent necessary for DocuSign: (a) to provide the DocuSign Services; (b) to verify Customer's compliance with the restrictions set forth in Section 2.2 (Restrictions) if DocuSign has a reasonable belief of Customer's non-compliance; and (c) as otherwise set forth in this Agreement. Noting in this Section 4.2 shall be construed to relieve DocuSign of its obligations to maintain the privacy and security of Customer Data as required by this MSA or any Service Schedule

4.3 Use of Aggregate Data. Customer agrees that DocuSign may collect, use, and disclose quantitative data derived from the use of the DocuSign Services for its business purposes, including industry analysis, benchmarking, analytics, and marketing. All data collected, used, and disclosed will be in aggregate and deidentified form only and will not identify Customer, its Authorized Users, Customer Data, or any third parties utilizing the DocuSign Services.

## 5. DISCOUNTS; PAYMENT OF FEES

5.1 Fees. Customer will pay Reseller for the DocuSign Services as set forth in the Reseller Agreement.

## 6. TAXES

6.1 Tax Responsibility. All payments required by this Agreement are stated exclusive of all taxes, duties, levies, imposts, fines or similar governmental assessments, including sales and use taxes, value-added taxes ("VAT"), goods and services taxes ("GST"), excise, business, service, and similar transactional taxes imposed by any jurisdiction and the interest and penalties thereon (collectively, "Taxes"). Customer shall be responsible for and bear Taxes for which it is responsible in accordance with applicable law and that are associated with its purchase of, payment for, access to or use of the DocuSign Services. Taxes shall not be deducted from the payments to DocuSign, except as required by law. If Customer claims tax exempt status for amounts due under this Agreement, it shall provide DocuSign with a valid tax exemption certificate (authorized by the applicable governmental authority) to avoid application of Taxes to Customer's invoice. Each Party is responsible for and shall bear Taxes imposed on its net income. Customer hereby confirms that DocuSign can rely on the ship-to name and address set forth in the Order Form(s) or SOW Customer places directly with DocuSign as being the place of supply for Tax purposes. The Parties' obligations under this Section 6.1 (Tax Responsibility) shall survive the termination or expiration of this Agreement.

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

## 7. TERM AND TERMINATION

7.1 Term. The term of an Order Form and any associated Service Schedule(s) is the period of time, including all renewals thereto, that begins on the Order Start Date and, unless terminated

sooner as provided herein, will continue until the Order End Date, both dates as specified on the Order Form (the "Term"). In the case of a SOW for Professional Services, if no end date is specified in the SOW, then the Term shall end upon completion and acceptance of Professional Services or early termination as permitted by this Agreement. Termination or expiration of any Order Form or SOW (i.e., a different Agreement) shall leave other Order Forms or SOWs unaffected.

**7.2 Termination for Breach; Termination for Insolvency.** If either Party commits a material breach or default in the performance of any of its obligations under this Agreement, then the other Party may terminate this Agreement in its entirety by giving the defaulting Party written notice of termination, unless the material breach or default in performance is cured within thirty (30) days after the defaulting Party receives notice thereof. Either Party may terminate this Agreement in its entirety upon written notice if the other Party becomes the subject of a petition in bankruptcy or any proceeding related to its insolvency, receivership or liquidation, in any jurisdiction, that is not dismissed within sixty (60) days of its commencement, or an assignment for the benefit of creditors.

**7.3 Post-Termination Obligations.** If this Agreement expires or is terminated for any reason: (a) Customer will pay to DocuSign any undisputed amounts that have accrued before, and remain unpaid as of, the effective date of the expiration or termination; (b) any and all liabilities of either Party to the other Party that have accrued before the effective date of the expiration or termination will survive; (c) licenses and use rights granted to Customer with respect to DocuSign Services and intellectual property will immediately terminate; (d) DocuSign's obligation to provide any further services to Customer under this Agreement will immediately terminate, except any such services that are expressly to be provided following the expiration or termination of this Agreement; and (e) the Parties' rights and obligations under Sections 6.1, 7.3, 8.3, and 10 through 13 will survive.

**7.5 Termination for Loss of Funding.** Without limiting Customer's right to terminate an Agreement pursuant to Section 7.2, nothing in this Agreement may be construed to permit any violation of Article XI, Section 7 of the Oregon Constitution or any other law regulating liabilities or monetary obligations of the State of Oregon. Customer's payment for services performed or license fees due after the last Calendar Day of the current biennium is contingent upon Customer receiving funding, appropriations, limitations, allotments or other expenditure authority from the Oregon Legislative Assembly (including its Emergency Board) sufficient to allow Customer, in the exercise of its reasonable administrative discretion, to continue to compensate DocuSign. Customer may immediately terminate this Agreement upon written notice if Customer fails to receive funding, appropriations, limitations, allotments, or other expenditure authority as contemplated by Customer's budget or spending plan and Customer determines, in its assessment and ranking of the policy objectives explicit or implicit in its budget or spending plan, that it is necessary to terminate this Agreement.

## 8. WARRANTIES AND DISCLAIMERS

**8.1 DocuSign Service Warranties.** DocuSign warrants that during the applicable Term, the DocuSign Services, when used as authorized under this Agreement, will perform substantially in conformance with the Documentation associated with the applicable DocuSign Services. Customer's sole and exclusive remedy for any breach of this warranty by DocuSign is for DocuSign to repair or replace the affected DocuSign Services to make them conform, or, if

DocuSign determines that the foregoing remedy is not commercially reasonable, then either Party may terminate this Agreement.

8.2 Mutual Warranties. Each Party represents and warrants that: (a) this Agreement has been duly executed and delivered and constitutes a valid and binding agreement enforceable against it in accordance with the terms of this Agreement; and (b) no authorization or approval from any third party is required in connection with its execution, delivery, or performance of this Agreement.

8.3 Disclaimer. Except for the express representations and warranties stated in this Section 8 (Warranties and Disclaimers), SOW or a Service Schedule, DocuSign: (a) makes no additional representation or warranty of any kind -- whether express, implied in fact or by operation of law, or statutory -- as to any matter whatsoever; (b) disclaims all implied warranties, including but not limited to merchantability, fitness for a particular purpose, and title; and (c) does not warrant that the DocuSign Services are or will be error-free or meet Customer's requirements. Customer has no right to make or pass on any representation or warranty on behalf of DocuSign to any third party.

## 9. THIRD-PARTY CLAIMS

9.1 By DocuSign. DocuSign will indemnify Customer, and its employees, directors, agents, and representatives from, and defend the Indemnified Parties against, any actual or threatened: (a) third-party claim; (b) third-party legal action; or (c) administrative agency action or proceeding ("Claim") to the extent arising from or related to: (i) any alleged breach by DocuSign of specified security safeguards related to the DocuSign Services that results in the breach of its confidentiality obligations in Section 11 (Confidentiality); and (ii) any alleged infringement of any third-party intellectual property rights by the DocuSign Services as provided by DocuSign, or the Indemnified Party's use thereof when used as authorized under this Agreement, provided, however, that DocuSign will not be responsible for alleged infringement that is solely due to the combination of DocuSign Services with goods or services provided by third parties.

9.2 By Customer. Subject to the limitations of Article XI, Section 7, of the Oregon Constitution and the Oregon Tort Claims Act (ORS 30.260 through 30.300) Customer will indemnify DocuSign, and its employees, directors, agents, and representatives from, and defend the Indemnified Parties against, any Claim to the extent arising from or related to: (a) use of the DocuSign Services by Customer or its Account Administrator or Authorized Users in violation of applicable law; (b) any breach by Customer of its obligations under Section 2.2 (e)-(h) (Restrictions) or Section 11 (Confidentiality); or (c) the nature and content of all Customer Data processed by the DocuSign Services.

9.3 Procedures. The Parties' respective indemnification obligations above are conditioned on: (a) the Indemnified Parties giving the Indemnifying Party prompt written notice of the Claim, except that the failure to provide prompt notice will only limit the indemnification obligations to the extent the Indemnifying Party is prejudiced by the delay or failure; (b) subject to Section 9.5, the Indemnifying Party being given full and complete control over the defense and settlement of the Claim (as long as the settlement does not include any payment of any amounts by or any admissions of liability, whether civil or criminal, on the part of any of the Indemnified Parties); (c) the relevant Indemnified Parties providing assistance in connection with the defense and settlement of the Claim, as the Indemnifying Party may reasonably request; and (d) the

Indemnified Parties' compliance with any settlement or court order made in connection with the Claim. The Indemnifying Party will indemnify the Indemnified Parties against: (i) all damages, costs, and attorneys' fees finally awarded against any of them with respect to any Claim; (ii) all out-of-pocket costs (including reasonable attorneys' fees) reasonably incurred by any of them in connection with the defense of the Claim (other than attorneys' fees and costs incurred without the Indemnifying Party's consent after it has accepted defense of such Claim); and (iii) all amounts that the Indemnifying Party agreed to pay to any third party in settlement of any Claims arising under this Section 9 (Third-Party Claims) and settled by the Indemnifying Party or with its approval.

**9.4 Infringement Remedy.** If Customer is enjoined or otherwise prohibited from using any of the DocuSign Services or a portion thereof based on a Claim covered by DocuSign's indemnification obligations under Section 9.1 (By DocuSign) above, then DocuSign will, at its sole expense and option, either: (a) obtain for Customer the right to use the allegedly infringing portions of the DocuSign Services; (b) modify the allegedly infringing portions of the DocuSign Services so as to render them non-infringing without substantially diminishing or impairing their functionality; or (c) replace the allegedly infringing portions of the DocuSign Services with non-infringing items of substantially similar functionality. If DocuSign determines that the foregoing remedies are not commercially reasonable, then either Party may terminate this Agreement, and in such case, DocuSign will provide a prorated refund to Customer for any prepaid fees received by DocuSign under this Agreement that correspond to the unused portion of the Term. Without limiting DocuSign's obligation to indemnify Customer as set forth in Section 9.1 (By DocuSign) above, the remedy set out in this Section 9.4 (Infringement Remedy) is Customer's sole and exclusive remedy for any actual or alleged infringement by DocuSign of any third-party intellectual property rights in the event that Customer is enjoined or otherwise prohibited from using any of the DocuSign Services or a portion thereof based on a Claim covered by DocuSign's indemnification obligations under Section 9.1 (By DocuSign).

**9.5 Approval of Counsel.** DocuSign will have control of the defense and settlement of any claim that is subject to Section 9.1 and for which the State of Oregon is the Indemnified Party; however, neither DocuSign nor any attorney engaged by DocuSign will defend such claim in the name of the State of Oregon or any agency of the State of Oregon, nor purport to act as legal representative of the State of Oregon or any of its agencies, without the approval of the Attorney General, nor will DocuSign settle any claim on behalf of the State of Oregon without the approval of the Attorney General. The State of Oregon may, at its election and expense, assume its own defense and settlement in the event that the State of Oregon determines that DocuSign is prohibited from defending the State of Oregon, is not adequately defending the State of Oregon's interests, or that an important governmental principle is at issue and the State of Oregon desires to assume its own defense.

## 10. LIMITATIONS OF LIABILITY

**10.1 Exclusion of Damages.** EXCEPT FOR THE PARTIES' OBLIGATIONS UNDER SECTION 9 (THIRD-PARTY CLAIMS), UNDER NO CIRCUMSTANCES, AND REGARDLESS OF THE NATURE OF THE CLAIM, SHALL EITHER PARTY (OR THEIR RESPECTIVE AFFILIATES) BE LIABLE TO THE OTHER PARTY FOR LOSS OF PROFITS, SALES OR BUSINESS, LOSS OF ANTICIPATED SAVINGS, LOSS OF USE OR CORRUPTION OF SOFTWARE, DATA OR INFORMATION, WORK STOPPAGE OR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, COVER, PUNITIVE, OR EXEMPLARY DAMAGES

ARISING OUT OF OR RELATED TO THE TRANSACTIONS CONTEMPLATED UNDER THIS AGREEMENT, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH LOSSES.

10.2 **Limitation of Liability.** EXCEPT FOR: (A) THE PARTIES' OBLIGATIONS UNDER SECTION 9 (THIRD-PARTY CLAIMS); (B) DAMAGES RESULTING FROM DEATH OR BODILY INJURY ARISING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; AND (C) UNPAID FEES DUE HEREUNDER, TO THE EXTENT PERMITTED BY LAW, THE TOTAL, CUMULATIVE LIABILITY OF EACH PARTY (OR THEIR RESPECTIVE AFFILIATES) ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE SERVICES PROVIDED HEREUNDER WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL BE LIMITED TO THE AMOUNTS DUE TO DOCUSIGN FOR THE DOCUSIGN SERVICE(S) GIVING RISE TO THE CLAIM DURING THE TERM OF THE EVENT GIVING RISE TO LIABILITY. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THIS CUMULATIVE LIMIT, HOWEVER THIS LIMIT WILL APPLY TO EACH AGREEMENT INDEPENDENT OF OTHER AGREEMENTS. THE PARTIES FURTHER ACKNOWLEDGE THAT CUSTOMER MAY HAVE STATUTORY RIGHTS AGAINST DOCUSIGN FRANCE SAS AND CUSTOMER ACKNOWLEDGES AND AGREES THAT ANY AMOUNTS RECOVERED BY CUSTOMER AGAINST DOCUSIGN FRANCE SAS PURSUANT TO SUCH RIGHTS SHALL BE AGGREGATED WITH ANY OTHER CLAIMS HEREUNDER FOR PURPOSES OF THE CAP ON DAMAGES SET FORTH ABOVE.

10.3 **Independent Allocations of Risk.** Each provision of this Agreement that provides for a limitation of liability, disclaimer of warranties, or exclusion of damages represents an agreed allocation of the risks of this Agreement between the Parties. This allocation is reflected in the pricing offered by DocuSign to Customer and is an essential element of the basis of the bargain between the Parties. Each of these provisions is severable and independent of all other provisions of this Agreement, and each of these provisions will apply even if the warranties in this Agreement have failed of their essential purpose.

## 11. CONFIDENTIALITY

11.1 **Restricted Use and Nondisclosure.** During and after the Term, Recipient will: (a) use the Confidential Information of the other Party solely for the purpose for which it is provided; (b) not disclose such Confidential Information to a third party, except on a need-to-know basis to its Affiliates, attorneys, auditors, consultants, and service providers who are under confidentiality obligations at least as restrictive as those contained herein; and (c) protect such Confidential Information from unauthorized use and disclosure to the same extent (but using no less than a reasonable degree of care) that it protects its own Confidential Information of a similar nature.

11.2 **Required Disclosure.** If Recipient is required by law to disclose Confidential Information of the other Party or the terms of this Agreement, Recipient will give prompt written notice to the other Party before making the disclosure, unless prohibited from doing so by the legal or administrative process, and cooperate with the disclosing Party to obtain where reasonably available an order protecting the Confidential Information from public disclosure.

11.3 **Ownership.** Recipient acknowledges that, as between the Parties, all Confidential Information it receives from the disclosing Party, including all copies thereof in Recipient's possession or control, in any media, is proprietary to and exclusively owned by the disclosing Party. Nothing in this Agreement grants Recipient any right, title or interest in or to any of the

disclosing Party's Confidential Information. Recipient's incorporation of the disclosing Party's Confidential Information into any of its own materials will not render Confidential Information non-confidential.

11.4 Remedies. Recipient acknowledges that any actual or threatened breach of this Section 11 (Confidentiality) may cause irreparable, non-monetary injury to the disclosing Party, the extent of which may be difficult to ascertain. Accordingly, the disclosing Party is entitled to (but not required to) seek injunctive relief in addition to all remedies available to the disclosing Party at law and/or in equity, to prevent or mitigate any breaches of this Agreement or damages that may otherwise result from those breaches. Absent written consent of the disclosing Party to the disclosure, the Recipient, in the case of a breach of this Section 11 (Confidentiality), has the burden of proving that the disclosing Party's Confidential Information is not, or is no longer, confidential or a trade secret and that the disclosure does not otherwise violate this Section 11 (Confidentiality).

11.5 Public Records. Notwithstanding any term to the contrary in this Agreement, Customer may disclose Confidential Information to the extent permitted by the Oregon Public Records Law, ORS 192.311 through 192.431.

## 12. GOVERNING LAW AND VENUE

12.1. Litigation. Any claim, action, suit, or proceeding (collectively, "Claim") between Customer (or any other agency or department of the State of Oregon) and DocuSign that arises from or relates to this Agreement must be brought and conducted solely and exclusively within the Circuit Court of Marion County for the State of Oregon. DOCUSIGN HEREBY CONSENTS TO THE IN PERSONAM JURISDICTION OF THE COURTS REFERENCED IN THIS SECTION 12.1. In no event may this Section be construed as (i) a waiver by the State of Oregon of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the eleventh amendment to the Constitution of the United States or otherwise, from any claim, or (ii) consent by the State of Oregon to the jurisdiction of any court.

12.2. Governing Law. This Agreement is governed by and construed according to the Laws of the State of Oregon without regard to principles of conflict of laws.

12.3 Attorneys Fees. Neither Party to this Agreement is entitled to obtain judgment from the other party for attorneys' fees incurred in any litigation between the Parties. 12.2 To the extent allowed by law, the English version of this Agreement is binding and other translations are for convenience only.

## 13. GENERAL

13.1 Relationship. The Parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the Parties. Except as set forth in this Agreement, nothing in this Agreement, expressed or implied is intended to give rise to any third-party beneficiary.

13.2 Assignability. Neither Party may assign its rights or obligations under this Agreement without the other Party's prior written consent. Notwithstanding the foregoing, either Party may assign its rights and obligations under this Agreement to an Affiliate as part of a reorganization, or to a purchaser of its business entity or substantially all of its assets or business to which rights and obligations pertain without the other Party's consent, provided that: (a) the purchaser is not insolvent or otherwise unable to pay its debts as they become due; (b) the purchaser is not a competitor of the other Party; and (c) any assignee is bound hereby. Other than the foregoing, any attempt by either Party to transfer its rights or obligations under this Agreement will be void.

13.3 Notices. Any notice required or permitted to be given in accordance with this Agreement will be effective only if it is in writing and sent using: (a) DocuSign Services; (b) certified or registered mail; or (c) a nationally recognized overnight courier, to the appropriate Party at the address set forth on the Order Form, with a copy, in the case of DocuSign, to [legal@docusign.com](mailto:legal@docusign.com). Each Party hereto expressly consents to service of process by registered mail. Either Party may change its address for receipt of notice by notice to the other Party through a notice provided in accordance with this Section 13.3 (Notices). Notices are deemed given upon receipt if delivered using DocuSign Services, two (2) business days following the date of mailing, or one (1) business day following delivery to a courier.

13.4 Force Majeure. In the event that either Party is prevented from performing, or is unable to perform, any of its obligations under this Agreement due to any cause beyond the reasonable control of the Party invoking this provision (including, without limitation, for causes due to war, fire, earthquake, flood, hurricane, riots, acts of God, telecommunications outage not caused by the obligated Party, or other similar causes) ("Force Majeure Event"), the affected Party's performance will be excused and the time for performance will be extended for the period of delay or inability to perform due to such occurrence; provided that the affected Party: (a) provides the other Party with prompt notice of the nature and expected duration of the Force Majeure Event; (b) uses commercially reasonable efforts to address and mitigate the cause and effect of such Force Majeure Event; (c) provides periodic notice of relevant developments; and (d) provides prompt notice of the end of such Force Majeure Event. Obligations to pay are excused only to the extent that payments are entirely prevented by the Force Majeure Event.

13.5 Export Control. The DocuSign Services, Documentation, and the provision and derivatives thereof are subject to the export control and sanctions laws and regulations of the United States and other countries that may prohibit or restrict access by certain persons or from certain countries or territories ("Trade Restrictions").

(a) Each Party shall comply with all applicable Trade Restrictions. In addition, each Party represents that it is not a Restricted Party, nor is it owned or controlled by, or acting on behalf of any person or entity that is a Restricted Party. "Restricted Party" means any person or entity that is: (a) listed on any U.S. government list of persons or entities with which U.S. persons are prohibited from transacting, including, but not limited to, OFAC's List of Specially Designated Nationals and Other Blocked Persons, the U.S. State Department's Nonproliferation Sanctions lists, the U.S. Commerce Department's Entity List or Denied Persons List located at <https://www.export.gov/article?id=Consolidated-Screening-List>; or (b) subject to end destination export control regulations, such as, but not limited to, the U.S. Export Administration Regulations and EU Dual-Use Regulation EC 428/2009.



(b) Customer acknowledges and agrees that it is solely responsible for complying with, and shall comply with, Trade Restrictions applicable to any of its own or its Affiliates' or Authorized Users' content or Customer Data transmitted through the DocuSign Services. Customer shall not and shall not permit any Authorized User to access, use, or make the DocuSign Services available to or by any Restricted Party or to or from within in a country or territory subject to comprehensive U.S. sanctions (currently including, but not limited to, Cuba, the Crimea region of the Ukraine, Iran, North Korea, and Syria).

13.6 Anti-Corruption. In connection with the services performed under this Agreement and Customer's use of DocuSign's products and services, the Parties agree to comply with all applicable anti-corruption and anti-bribery related laws, statutes, and regulations.

13.7 U.S. Government Rights. All DocuSign software (including DocuSign Services) is commercial computer software and all services are commercial items. "Commercial computer software" has the meaning set forth in Federal Acquisition Regulation ("FAR") 2.101 for civilian agency purchases and the Department of Defense ("DOD") FAR Supplement ("DFARS") 252.227-7014(a)(1) for defense agency purchases. If the software is licensed or the DocuSign Services are acquired by or on behalf of a civilian agency, DocuSign provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as required in FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data) and their successors. If the software is licensed or the DocuSign Services are acquired by or on behalf of any agency within the DOD, DocuSign provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as specified in DFARS 227.7202-3 and its successors. Only if this is a DOD prime contract or DOD subcontract, the Government acquires additional rights in technical data as set forth in DFARS 252.227-7015. Except as otherwise set forth in an applicable Service Schedule, this Section 13.7 (U.S. Government Rights) is in lieu of, and supersedes, any other FAR, DFARS or other clause or provision that addresses U.S. Government rights in computer software or technical data.

13.8 Publicity. Neither Party shall refer to the identity of the other Party in promotional material, publications, or press releases or other forms of publicity relating to the DocuSign Service unless the prior written consent of the other Party has been obtained.

13.9 Waiver. The waiver by either Party of any breach of any provision of this Agreement does not waive any other breach. The failure of any Party to insist on strict performance of any covenant or obligation in accordance with this Agreement will not be a waiver of such Party's right to demand strict compliance in the future, nor will the same be construed as a novation of this Agreement.

13.10 Severability. If any part of this Agreement is found to be illegal, unenforceable, or invalid, the remaining portions of this Agreement will remain in full force and effect.

13.11 Entire Agreement. This Agreement is the final, complete, and exclusive expression of the agreement between the Parties regarding the DocuSign Services provided under this Agreement. This Agreement supersedes and replaces, and the Parties disclaim any reliance on, all previous oral and written communications (including any confidentiality agreements pertaining to the DocuSign Services under this Agreement), representations, proposals, understandings,

undertakings, and negotiations with respect to the subject matter hereof and apply to the exclusion of any other terms that Customer seeks to impose or incorporate, or which are implied by trade, custom, practice, or course of dealing. This Agreement may be changed only by a written agreement signed by an authorized agent of both Parties. This Agreement will prevail over terms and conditions of any Customer-issued purchase order or other ordering documents, which will have no force and effect, even if DocuSign accepts or does not otherwise reject the purchase order or other ordering document.

### **13.12 Additional Provisions.**

(a) Incorporation of Oregon Statutes. To the extent legally required, ORS 279B.220, 279B.230 and 279B.235 are incorporated into this Agreement by reference, as applicable to the Agreement.

(b) Compliance with Oregon Statutes. DocuSign represents that, to the best of its knowledge, it is not in violation of any Oregon Statutes, and will comply with such Statutes to the extent those Statutes are applicable to the products and services to be provided by DocuSign.

(c) Tax Compliance. To the extent legally required, DocuSign represents and warrants that it has complied with the tax laws of the State of Oregon or a political subdivision of the State of Oregon, including but not limited to ORS 305.620 and ORS chapters 316, 317 and 318. DocuSign will continue to comply with the tax laws of the State of Oregon or a political subdivision of the State of Oregon during the term of this Agreement. If DocuSign failed or fails to comply the tax laws of the State of Oregon or a political subdivision of the State of Oregon before the effective date of this Agreement or during the term of this Agreement, DocuSign will be in default, and Customer may terminate this Agreement and seek damages and other relief available under the terms of this Agreement under applicable law.

(d) Tax Compliance Certificate. The individual signing this Agreement for DocuSign certifies under penalty of perjury that he or she is authorized to act on behalf of DocuSign and that, to the best of the undersigned's knowledge, DocuSign is not in violation of any Oregon Tax Laws. For purposes of this certification, "Oregon Tax Laws" means a state tax imposed by ORS 403.200 to 403.250 (Tax For Emergency Communications), chapters 118 (Inheritance Tax), 314 (Income Tax), 316 (Personal Income Tax), 317 (Corporation Excise Tax), 318 (Corporation Income Tax), and 323 (Cigarettes And Tobacco Products Tax), and the elderly rental assistance program under ORS 310.630 to 310.706; and the taxes of any political subdivision of the State of Oregon, including any local taxes administered by the Department of Revenue under ORS 305.620.

(e) Funding. Nothing in this Agreement may be construed to permit any violation of Article XI, Section 7 of the Oregon Constitution or any other law regulating liabilities or monetary obligations of the State of Oregon.

(f) Anti-Discrimination. DocuSign certifies that DocuSign has a written policy and practice that meets the requirements described in ORS 279A.212 for preventing sexual harassment, sexual assault, and discrimination against employees who are members of a protected class. DocuSign agrees, as a material term of this Agreement, to maintain such policy and practice in force during the entire term of this Agreement. DocuSign's failure to maintain such policy and practice constitutes a breach entitling Customer to terminate this Agreement for cause.

(g) Pay Equity. As required by ORS 279B.235, DocuSign shall comply with ORS 652.220 and not unlawfully discriminate against any of its employees in the payment of wages or other compensation for work of comparable character based on an employee's membership in a protected class. "Protected class" means a group of persons distinguished by race, color, religion, sex, sexual orientation, national origin, marital status, veteran status, disability, or age. DocuSign's compliance with this section is a material term of this Agreement, and DocuSign's failure to comply constitutes a breach entitling Customer to terminate this Agreement for cause.

(h) Salary Information. As required by ORS 279B.235, DocuSign may not prohibit any of its employees from discussing the employee's rate of wage, salary, benefits, or other compensation with another employee or another person. DocuSign shall not retaliate against an employee who discusses the employee's rate of wage, salary, benefits, or other compensation with another employee or another person.

## ATTACHMENT II

# SERVICE SCHEDULE for DOCUSIGN SIGNATURE

Service Schedule revision date: August 1, 2019. Unless otherwise defined in this Service Schedule, capitalized terms will have the meaning given to them in the Agreement.

### 1. DEFINITIONS

“DocuSign Signature” means the on-demand electronic signature DocuSign Service, which provides online display, certified delivery, acknowledgement, electronic signature, and storage services for eDocuments via the Internet.

“Envelope” means an electronic record containing one or more eDocuments consisting of a single page or a group of pages of data uploaded to the System.

“Signer” means a person designated by an Authorized User to access and/or take action upon the eDocuments sent to such individual via DocuSign Signature.

“System” refers to the software systems and programs, the communication and network facilities, and the hardware and equipment used by DocuSign or its agents to make available the DocuSign Signature service via the Internet.

“Transaction Data” means the metadata associated with an Envelope (such as transaction history, image hash value, method and time of Envelope deletion, sender and recipient names, email addresses and signature IDs) that DocuSign may use to generate and maintain the digital audit trail required by DocuSign Signature.

### 2. ADDITIONAL USAGE LIMITATIONS AND CUSTOMER RESPONSIBILITIES

2.1 DocuSign’s provision of DocuSign Signature is conditioned on Customer’s acknowledgement of and agreement to the following:

(a) DocuSign Signature facilitates the execution of eDocuments between the parties to those eDocuments. Nothing in this Service Schedule may be construed to make DocuSign a party to any eDocument processed through DocuSign Signature, and DocuSign makes no representation or warranty regarding the transactions sought to be effected by any eDocument;

(b) Between DocuSign and Customer, Customer has exclusive control over and responsibility for the content, quality, and format of any eDocument. Without limiting the foregoing, all eDocuments, together with any messages included within an Envelope, stored by DocuSign on the System are maintained in an encrypted form, and DocuSign has no control of or access to their contents except to the extent access is requested in writing and made available by Customer to DocuSign;

(c) Certain types of agreements and documents may be excepted from electronic signature laws (e.g. wills and agreements pertaining to family law) or may be subject to specific regulations promulgated by various government agencies regarding electronic signatures and electronic records. DocuSign is not responsible or liable to determine whether any particular eDocument is subject to an exception to applicable electronic signature laws, or whether it is subject to any particular agency promulgations, or whether it can be legally formed by electronic signatures;

(d) DocuSign is not responsible for determining how long any contracts, documents, and other records are required to be retained or stored under any applicable laws, regulations, or legal or administrative agency processes. Further, DocuSign is not responsible for or liable to produce any of Customer's eDocuments or other documents to any third parties;

(e) Certain consumer protection or similar laws or regulations may impose special requirements with respect to electronic transactions involving one or more "consumers," such as (among others) requirements that the consumer consent to the method of contracting and/or that the consumer be provided with a copy, or access to a copy, of a paper or other non-electronic, written record of the transaction. DocuSign does not and is not responsible to: (i) determine whether any particular transaction involves a "consumer"; (ii) furnish or obtain any such consents or determine if any such consents have been withdrawn; (iii) provide any information or disclosures in connection with any attempt to obtain any such consents; (iv) provide legal review of, or update or correct any information or disclosures currently or previously given; (v) provide any such copies or access, except as expressly provided in the Documentation for all transactions, consumer or otherwise; or (vi) comply with any such special requirements;

(f) Customer undertakes to determine whether any "consumer" is involved in any eDocument presented by its Authorized Users for processing, and, if so, to comply with all requirements imposed by law on such eDocuments or their formation;

(g) Customer agrees that its assigned Account Administrator has authority to provide DocuSign with any required authorizations, requests, or consents on behalf of Customer with respect to Customer's Account; and

(h) Customer agrees it is solely responsible for the accuracy and appropriateness of instructions given by it and its personnel to DocuSign in relation to the Services, including without limitation instructions through its Account as made by the assigned Account Administrator.

### 3. eDOCUMENT STORAGE AND DELETION

3.1 During the Term. Customer may retrieve electronic copies of its stored eDocuments at any time while this Service Schedule is in effect at no additional cost. DocuSign will store all completed eDocuments sent by Customer during the Term and for a period of no less than 90 days following the end of the Term, by default. However, Customer has the option through its Account Administrator to change its Account settings to direct the deletion of all or certain designated eDocuments at an earlier date or periodic interval. If Customer fails to retrieve its eDocuments prior to the expiration or termination of the Service Schedule, Customer may request, no later than ninety (90) days after such expiration or termination, that DocuSign provide Professional Services to assist in retrieving completed eDocuments still remaining in the System, the details of which Professional Services will be set out in a SOW. After such ninety (90)-day period, DocuSign

shall have no obligation to maintain or provide any eDocuments and DocuSign shall have the right to delete all eDocuments in the System or otherwise in its possession or under its control and delete Customer's Account.

3.2 DocuSign may retain Transaction Data for as long as it has a business purpose to do so, provided that any Transaction Data that constitutes Confidential Information of Customer will at all times maintain that status, and DocuSign will comply with its confidentiality obligations as provided in the Agreement.

#### 4. INFORMATION SECURITY AND DATA PROCESSING

4.1 Security. DocuSign will use commercially reasonable technical and organizational measures designed to prevent unlawful or unauthorized access, use, alteration, or disclosure of Customer Data in accordance with the provisions of DocuSign's Security Attachment for DocuSign Signature attached hereto. [attached](#).

#### 5. SUBSCRIPTION PLANS AND FEES

DocuSign Signature is made available based on a prepaid subscription, which is subject to the restrictions set forth in the applicable Order Form.

5.1 "Seat Allowance" means the maximum number of Authorized Users ("Seats") that Customer may have active in its Account as assigned by Customer's Account Administrator. For purposes of determining usage of Seats:

(a) The number of Seats in use is determined by the total number of Authorized Users registered in Customer's Account with access to DocuSign Signature at any time during the Term.

(b) No two individuals may log onto or use DocuSign Signature as the same Authorized User, but Customer through its Account Administrator may unregister or deactivate Authorized Users and replace them with other Authorized Users without penalty, so long as the number of active Authorized Users registered at any one time does not exceed the number of Seats purchased.

5.2 "Envelope Allowance" means the cumulative number of Envelopes that may be sent by Authorized Users registered in Customer's Account. There is no individual limit on number of Envelopes that may be sent by each Authorized User, so long as the total volume sent by all Authorized Users does not exceed the Envelope Allowance. For purposes of calculating Envelope usage:

(a) An Envelope is consumed when sent by an Authorized User, regardless of whether the Envelope has been received by any recipients or whether any recipients have performed any actions upon any eDocument in the Envelope;

(b) Usage of a Powerform will be applied against the Envelope Allowance. A Powerform will be deemed consumed at the time it is accessed by any user regardless of whether any actions are subsequently performed upon such Envelope. "Powerform" means an Envelope that may be accessed and completed by accessing a hyperlink (i.e. which does not need to be individually sent to each recipient);

(c) An Envelope sent via bulk send or automated batch sending, including through a DocuSign API, will be applied against the Envelope Allowance.

5.3 Calculation of Envelope Allowance. Unless otherwise set forth in the Order Form, the Envelope Allowance for each twelve (12)-month period during the Order Term is calculated by multiplying the Seat Allowance times one hundred (100) Envelopes. For example, a three (3)-year subscription for ten (10) Seats would result in an Envelope Allowance of one thousand (1000) Envelopes per year. An Envelope Allowance may be augmented by purchasing additional Seats (each of which supply an additional one hundred (100) Envelopes unless otherwise set forth in the Order Form) or additional batches of Envelopes, pursuant to an Order Form.

5.4 Overage.

(a) Seats. If Customer through its Account Administrator adds more Authorized Users than the amount permitted under the Seat Allowance, then Customer hereby agrees that additional charges of one Seat per additional Authorized User for the remainder of the Order Term will become immediately due and payable. Additional Seats will be charged as a pro-rata portion (calculated based on the amount of time remaining in the Order Term) of the then-current list price for Seats under the applicable subscription type, or such other amount as is specified in the Order Form, and will include a pro-rata allocation of Envelopes.

(b) Envelopes. Customer hereby agrees that all Envelopes sent in excess of the Envelope Allowance during the Term will incur a per-Envelope overage charge at the then-current list price for the applicable subscription type, or such other amount as is specified in the Order Form. Envelope overage charges will be invoiced monthly in arrears.

(c) Limitations. Customer's obligations under Sections 5.4(a) and (b) are subject to Section 13.12(e) of the MSA.

5.5 Optional features, such as Authentication Measures or fax-back services, may be purchased on a subscription or per-use basis, as set forth in the Order Form.

## 6. DOCUSIGN PAYMENTS

6.1 DocuSign Signature may be ordered with "DocuSign Payments," which means functionality that allows Customer to submit agreements, invoices, and other documents to Signers via DocuSign Signature to facilitate the submission of Signer payment credentials and authorizations directly to payment applications, gateways, processors, and service providers that store, process, or transmit cardholder data as part of authorization or settlement ("Payment Applications").

6.2 DocuSign's provision of DocuSign Payments is conditioned on Customer's acknowledgement of and agreement to the following:

(a) The payment processing activities facilitated through DocuSign Payments are between Customer and a Payment Application or another third party designated by Customer and not with DocuSign. Customer is solely responsible for registering and maintaining an account with Payment Applications to facilitate the payment processing via DocuSign Payments and for complying with all agreements, terms of use, or other terms and conditions between Customer and such Payment

Applications. Payment Applications are independent contractors and not agents, employees, or subcontractors of DocuSign. DocuSign does not control the payment methods (i.e., credit card, debit card, ACH transfer) made available by the Payment Applications through DocuSign Signature nor the products or services that are sold or purchased by Customer via DocuSign Payments. Customer acknowledges and agrees that DocuSign cannot ensure that a Payment Application Signer or third party will complete a payment processing or that it is authorized to do so.

(b) Customer authorizes DocuSign to store, process, and transmit Customer Data as necessary for a Payment Application to facilitate payment processing between Customer and a third party designated by Customer. DocuSign Payments will temporarily store information received from Customer, such as account information for a Payment Application, only to facilitate the payment processing.

(c) Customer is solely responsible for complying with: (1) any applicable standards developed and published by payment networks (such as Visa, Mastercard, American Express, and any other credit, debit, or electronic funds transfer network), including but not limited to, the current Payment Card Industry Data Security Standard (“PCI DSS”); and (2) all laws and regulations applicable to the payment processing conducted by Customer via DocuSign Payments, including but not limited to, those that may apply to Customer: in connection with collecting and storing information, including payment credentials about Signers; making adequate, clear, and conspicuous disclosures related to the storage and use of Signers’ payment credentials; and the use of stored payment credentials to collect future payments.

(d) Customer is solely responsible for any and all disputes with any Payment Applications or Signers related to or in connection with a payment processing sought to be facilitated via DocuSign Payments, including but not limited to: (1) chargebacks; (2) products or services not received; (3) return of, delayed delivery of, or cancelled products or services; (4) cancelled transactions; (5) duplicate transactions or charges; (6) electronic debits and credits involving bank accounts, debit cards, credit cards, and check issuances; and (7) the amount of time to complete payment processing.

6.3 To the extent applicable to the DocuSign Payments Service provided by DocuSign in the provision of DocuSign Payments, DocuSign represents that it is presently in compliance, and will remain in compliance, with the current PCI DSS Standard. DocuSign acknowledges that credit and debit card account numbers or related data processed via DocuSign Payments is, as applicable, owned exclusively by Customer, credit card issuers, the relevant payment networks, and entities licensed to process credit and debit card transactions on behalf of Customer, and further acknowledges that such information may be used by DocuSign solely to assist the foregoing parties in completing the processing activities described in the Agreement.

## 7. ADDITIONAL WARRANTIES AND DISCLAIMERS

7.1 Additional DocuSign Warranties. DocuSign warrants that: (a) DocuSign Signature will not introduce files, scripts, agents or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses (“Malicious Code”) into Customer's system; (b) the proper use of DocuSign Signature by Customer in accordance with the Documentation and applicable law will be sufficient to meet the definition of an “electronic signature” as defined in the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. ch. 96 §§ 7001 et seq. (the “ESIGN Act”);



and in Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (“eIDAS”).

7.2 DISCLAIMER. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN THIS SECTION 7 AND IN THE MSA, AND SUBJECT TO THE ADDITIONAL LIMITATIONS OF LIABILITY THEREIN, DOCUSIGN: (A) MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND -- WHETHER EXPRESS, IMPLIED IN FACT OR BY OPERATION OF LAW, OR STATUTORY -- AS TO ANY MATTER WHATSOEVER; (B) DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND THE LIKE; AND (C) DOES NOT WARRANT THAT DOCUSIGN SIGNATURE IS OR WILL BE UNINTERRUPTED OR ERROR-FREE OR MEET CUSTOMER’S REQUIREMENTS. CUSTOMER HAS NO RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTY ON BEHALF OF DOCUSIGN TO ANY THIRD PARTY.

# ATTACHMENT III

## SECURITY ATTACHMENT for DOCUSIGN SIGNATURE

Service Attachment version date: May 25, 2018

This Security Attachment for DocuSign Signature (“Security Attachment”) sets forth DocuSign’s commitments for the protection of Customer Data and is made part of the Service Schedule for DocuSign Signature. The terms of this Security Attachment are limited to the scope of the DocuSign Signature service and are not applicable to any other Service Schedules or DocuSign Services. Unless otherwise defined in this Security Attachment, capitalized terms will have the meaning given to them in the Agreement.

### 1. DEFINITIONS

“Personnel” means all employees and agents of DocuSign involved in the performance of DocuSign Signature service.

“Process” or “Processing” means, with respect to this Security Attachment, any operation or set of operations that is performed upon Customer Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

“Production Environment” means the System setting where software, hardware, data, processes, and programs are executed for their final and intended operations by end users of DocuSign Signature.

“Subcontractor” means a third party that DocuSign has engaged to perform all or a portion of the DocuSign Signature service on behalf of DocuSign.

### 2. INFORMATION SECURITY PROGRAM

2.1 Information Security Program. DocuSign maintains and will continue to maintain a written information security program that includes policies, procedures, and controls governing the Processing of Customer Data through DocuSign Signature (the “Information Security Program”). The Information Security Program is designed to protect the confidentiality, integrity, and availability of Customer Data by using a multi-tiered technical, procedural, and people-related control approach in accordance with industry best practices and applicable laws and regulations, including the Oregon Consumer Information Protection Act, ORS 646A.600 to 646A.628.

2.2 Permitted Use of Customer Data. DocuSign will not Process Customer Data in any manner other than as permitted or required by the Agreement.

**2.3 Acknowledgement of Shared Responsibilities.** The security of data and information that is accessed, stored, shared, or otherwise Processed via a multi-tenant cloud service such as DocuSign Signature are shared responsibilities between a cloud service provider and its customers. As such, the Parties acknowledge that: (a) DocuSign is responsible for the implementation and operation of the Information Security Program and the protection measures described in the Agreement and this Security Attachment; and (b) Customer is responsible for properly implementing access and use controls and configuring certain features and functionalities of DocuSign Signature that Customer may elect to use DocuSign Signature in the manner that Customer deems adequate to maintain appropriate security, protection, deletion, and backup of Customer Data.

**2.4 Applicability to Customer Data.** This Security Attachment and the Information Security Program apply specifically to the Customer Data Processed via DocuSign Signature. To the extent Customer exchanges data and information with DocuSign that does not meet the definition of "Customer Data," DocuSign will treat such data and information in accordance with the confidentiality terms set forth in the Agreement.

### 3. SECURITY MANAGEMENT

**3.1 Maintenance of Information Security Program.** DocuSign will take and implement appropriate technical and organizational measures to protect Customer Data located in DocuSign Signature and will maintain the Information Security Program in accordance with standards set forth in NIST Special Publication 800-53, Revision 5, and the State of Oregon 2019 Statewide Information and Cyber Security Standards located at <https://www.oregon.gov/das/OSCIO/Documents/2019StatewideInformationAndCyberSecurityStandardsV1.0.pdf>, or such other alternative standards that are substantially equivalent to the foregoing standards.. DocuSign may update or modify the Information Security Program from time to time provided that such updates and modifications comply with the standards set forth above, and do not result in the degradation of the overall security of DocuSign Signature.

**3.2 Background Checks and Training.** DocuSign will conduct reasonable and appropriate background investigations on all Personnel in accordance with applicable laws and regulations. Personnel must pass DocuSign's background checks prior to being assigned to positions in which they will, or DocuSign reasonably expects them to, have access to Customer Data. DocuSign will conduct annual mandatory security awareness training to inform its Personnel on procedures and policies relevant to the Information Security Program and of the consequences of violating such procedures and policies.

**3.3 Subcontractors.** DocuSign will evaluate all Subcontractors to ensure that Subcontractors maintain adequate physical, technical, organizational, and administrative controls, based on the risk tier appropriate to their subcontracted services, that support DocuSign's compliance with the requirements of the Agreement and this Security Attachment. All Subcontractors fall into scope for independent audit assessment as part of, or maintain an independent audit assessment which conforms to, DocuSign's ISO 27001 audit or an equivalent standard, where their roles and activities are reviewed per control requirements. DocuSign will remain responsible for the acts and omissions of its Subcontractors as they relate to the services performed under the Agreement as if it had performed the acts or omissions itself and any subcontracting will not reduce DocuSign's obligations to Customer under the Agreement.

3.4 Risk Management Plan. DocuSign shall maintain a documented security risk management plan and will provide Customer a copy of such plan upon request and notify Customer of any changes to the security risk management plan.

3.5 Location of Services and Customer Data. Except with the Customer's express written permission, the DocuSign Signature services (including storage and backup of Customer Data and disaster recovery services and infrastructure), shall be provided solely from within the continental United States and on computing and data storage devices residing therein. In the event DocuSign has secured the Customer's permission to perform some of the DocuSign Signature Services from outside the United States, DocuSign will comply with the Customer's reasonable written security requirements made as conditions of such permission.

3.6 Risk and Security Assurance Framework Contact. Customer's account management team at DocuSign will be Customer's first point of contact for information and support related to the Information Security Program. The DocuSign account management team will work directly with Customer to escalate Customer's questions, issues, and requests to DocuSign's internal teams as necessary.

#### 4. PHYSICAL SECURITY MEASURES

4.1 General. DocuSign will maintain appropriate physical security measures designed to protect the tangible items, such as physical computer systems, networks, servers, and devices, that Process Customer Data. DocuSign will utilize commercial grade security software and hardware to protect the DocuSign Signature service and the Production Environment.

4.2 Facility Access. DocuSign will ensure that: (a) access to DocuSign's corporate facilities is tightly controlled; (b) all visitors to its corporate facilities sign in, agree to confidentiality obligations, and be escorted by Personnel while on premises at all times; and (c) visitor logs are reviewed by DocuSign's security team on a regular basis. DocuSign will revoke Personnel's physical access to DocuSign's corporate facilities upon termination of employment.

4.3 Data Center Access. DocuSign will ensure that its commercial-grade data center service providers used in the provision of DocuSign Signature maintain an on-site security operation that is responsible for all physical data center security functions and formal physical access procedures in accordance with SOC1 and SOC 2, or equivalent, standards. DocuSign's data centers are included in DocuSign's ISO 27001 or equivalent certification.

#### 5. LOGICAL SECURITY

5.1 Access Controls. DocuSign will maintain a formal access control policy and employ a centralized access management system to control Personnel access to the Production Environment.

a. DocuSign will ensure that all access to the Production Environment is subject to successful two-factor authentication globally from both corporate and remote locations and is restricted to authorized Personnel who demonstrate a legitimate business need for such access. DocuSign will maintain an associated access control process for reviewing and implementing Personnel access requests. DocuSign will regularly review the access rights of authorized Personnel and, upon

change in scope of employment necessitating removal or employment termination, remove or modify such access rights as appropriate.

b. DocuSign will monitor and assess the efficacy of access restrictions applicable to the control of DocuSign's system administrators in the Production Environment, which will entail generating system individual administrator activity information and retaining such information for a period of at least 12 months.

**5.2 Network Security.** DocuSign will maintain a defense-in-depth approach to hardening the Production Environment against exposure and attack. DocuSign will maintain an isolated Production Environment that includes commercial grade network management controls such as load balancers, firewalls, intrusion detection systems distributed across production networks, and malware protections. DocuSign will complement its Production Environment architecture with prevention and detection technologies that monitor all activity generated and send risk-based alerts to the relevant security groups.

**5.3 Malicious Code Protection.** DocuSign will ensure that: (a) its information systems and file transfer operations have effective and operational anti-virus software; (b) all anti-virus software is configured for deployment and automatic update; and (c) applicable anti-virus software is integrated with processes and will automatically generate alerts to DocuSign's Cyber Incident Response Team if potentially harmful code is detected for their investigation and analysis.

**5.4 Code Reviews.** DocuSign will maintain a formal software development lifecycle that includes secure coding practices against OWASP and related standards and will perform both manual and automated code reviews. DocuSign's engineering, product development, and product operations management teams will review changes included in production releases to verify that developers have performed automated and manual code reviews designed to minimize associated risks. In the event that a significant issue is identified in a code review, such issue will be brought to DocuSign senior management's attention and will be closely monitored until resolution prior to release into the Production Environment.

**5.5 Vulnerability Scans and Penetration Tests.** DocuSign will perform both internal and external vulnerability scanning and application scanning. Quarterly external scans and annual penetration tests against DocuSign Signature and the Production Environment will be conducted by external qualified, credentialed, and industry recognized organizations. DocuSign will remedy vulnerabilities identified during scans and penetration tests in a commercially reasonable manner and timeframe based on severity. Upon Customer's reasonable written request, DocuSign will provide third party attestations resulting from vulnerability scans and penetration tests per independent external audit reports. For clarification, under no circumstance will Customer be permitted to conduct any vulnerability scans or penetration testing against the Production Environment.

**5.6 Auditing and Logging.** With respect to system auditing and logging, DocuSign will do the following:

(a) DocuSign will use and maintain an auditing and logging mechanism that, at a minimum, captures and records successful and failed user logons and logoffs (with a date and time stamp, user ID, application name, and pass/fail indicator). User access activities will be logged and

audited periodically by DocuSign to identify unauthorized access and to determine possible flaws in DocuSign's access control system.

(b) All application components that have logging capabilities (such as operating systems, databases, web servers, and applications) will be configured to produce a security audit log.

(c) Audit logs will be configured for sufficient log storage capacity.

(d) Each log will be configured so that it cannot be disabled without proper authorization and will send alerts for the success or failure of each auditable event.

(e) Access to security log files will be limited to authorized Personnel, and to Customer upon request.

(f) In regard to DocuSign's development, access to source code by team members must be reviewed at least every ninety (90) days.

(g) In regard to DocuSign's support, DocuSign will maintain a process to help assure that any individual leaving DocuSign's team that provides support to Customer will lose access to Customer's accounts and data upon termination of employment or as soon as reasonably possible after moving to another position within DocuSign.

## 6. STORAGE, ENCRYPTION, AND DISPOSAL

6.1 Separation. DocuSign will logically separate Customer Data located in the Production Environment from other DocuSign customer data.

6.2 Encryption Technologies. DocuSign will encrypt Customer Data in accordance with industry best practice standards. All access and transfer of data to and from DocuSign Signature will be via HTTPS and DocuSign will only support industry recognized and best practice cipher suites. DocuSign will encrypt all eDocuments persisted on the Production Environment with an AES 256-bit, or equivalent, encryption key.

6.3 Return or Destruction of Customer Data and Other Customer Assets. At any time upon the Customer's demand DocuSign will promptly return to the Customer or destroy all Customer Data, files, records, documents, materials, and other items which contain any Data and all other Customer assets in DocuSign's possession or control. Any copies thereof shall also be returned. DocuSign will comply with this requirement with or without a termination of the Agreement. In the absence of such a demand, DocuSign will return or destroy in accordance with Section 6.4 all such Customer Data and other Customer assets upon the termination of the Contract. DocuSign's failure to comply with this subsection shall be a material breach of the Agreement.

6.4 Disposal. DocuSign will maintain a data disposal and re-use policy for managing assets and implement industry recognized processes and procedures for equipment management and secure media disposal, which includes erase, destroy, and render unrecoverable all Customer Data within 90 days after any termination of the Agreement. Media will be destroyed and rendered unrecoverable on DocuSign CLM in accordance with the standards identified in the National Institute of Standards' Guidelines for Media Sanitization, SP800-88.

## 7. BUSINESS CONTINUITY AND DISASTER RECOVERY

7.1 Continuity Plan. DocuSign will maintain a written business continuity and disaster recovery plan that addresses the availability of DocuSign Signature (“Continuity Plan”). The Continuity Plan will include elements such as: (a) crisis management, plan and team activation, event and communication process documentation; (b) business recovery, alternative site locations, and call tree testing; and (c) infrastructure, technology, system(s) details, recovery activities, and identification of the Personnel and teams required for such recovery. DocuSign will, at a minimum, conduct a test of the Continuity Plan on an annual basis.

7.2 DocuSign Signature Continuity. DocuSign’s production architecture for DocuSign Signature is designed to perform secure replication in near real-time to multiple active systems in geographically distributed and physically secure data centers. DocuSign will ensure that: (a) infrastructure systems for DocuSign Signature have been designed to eliminate single points of failure and to minimize the impact of anticipated environmental risks; (b) each data center supporting DocuSign Signature includes full redundancy and fault tolerance infrastructure for electrical, cooling, and network systems; and (c) Production Environment servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability.

## 8. INCIDENT RESPONSE AND BREACH NOTIFICATION

8.1 General. DocuSign will maintain a tested incident response program, which will be managed and run by DocuSign’s dedicated Global Incident Response Team. DocuSign’s Global Incident Response Team will operate to a mature framework that includes incident management and breach notification policies and associated processes. DocuSign’s incident response program will include, at a minimum, initial detection; initial tactical response; initial briefing; incident briefing; refined response; communication and message; formal containment; formal incident report; and post mortem/trend analysis.

8.2 Breach Notification. Unless notification is delayed by the actions or demands of a law enforcement agency, DocuSign shall report to Customer: (a) any unlawful access or unauthorized acquisition use, or disclosure of Customer Data persisted in DocuSign Signature (a “Data Breach”) within one calendar day following determination by DocuSign that a Data Breach has occurred. DocuSign’s obligation to report a Data Breach under this Security Attachment is not and will not be construed as an acknowledgement by DocuSign of any fault or liability of DocuSign with respect to such Data Breach.

8.3 Breach Response. DocuSign shall take reasonable measures to mitigate the cause of any Data Breach and shall take reasonable corrective measures to prevent future Data Breaches. As information is collected or otherwise becomes available to DocuSign and unless prohibited by law, DocuSign shall provide information regarding the nature and consequences of the Data Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Due to the encryption configuration and security controls associated with DocuSign Signature, DocuSign will not have access to or know the nature of the information contained within Customer’s eDocuments and, as such, the Parties acknowledge that it may not be possible for DocuSign to provide Customer with a description of the type of

information or the identity of individuals who may be affected by a Data Breach. Customer is solely responsible for determining whether to notify impacted individuals and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer's use of DocuSign Signature need to be notified of a Data Breach.

## 9. INDEPENDENT ASSURANCES AND AUDITS

9.1 Independent Assurances. DocuSign uses independent external auditors to verify the adequacy of its Information Security Program. Upon Customer's reasonable written request, DocuSign will provide Customer with third party attestations, certifications, and reports relevant to the establishment, implementation, and control of the Information Security Program, including DocuSign's ISO 27001 certification, PCI DSS certification, and Service Organization Controls (SOC) 2, Type 2 reports.

9.2 Regulatory Audit. If Customer's governmental regulators require that Customer perform an on-site audit of DocuSign's Information Security Program, as supported by evidence provided by Customer, Customer may at Customer's expense, either through itself or a third party independent contractor selected by Customer, conduct an on-site audit of DocuSign's Information Security Program, including DocuSign's data centers and corporate facilities relevant to the security of Customer Data ("Regulatory Audit"). Customer must submit any requests for an onsite Regulatory Audit to its DocuSign account management representative, who will work with DocuSign's internal teams to schedule such audit. If a Regulatory Audit requires the equivalent of more than one business day of DocuSign Personnel's time to support such audit, DocuSign may, at its discretion, charge Customer an audit fee at DocuSign's then-current rates, which will be made to Customer upon request, for each day thereafter.

9.3 Audit for Data Breach. Following a Data Breach, DocuSign will, upon Customer's written request, promptly engage a third party independent auditor, selected by DocuSign and at DocuSign's expense, to conduct an on-site audit of DocuSign's Information Security Program, including DocuSign's data centers and corporate facilities relevant to the security of Customer Data. DocuSign will promptly provide Customer with the report of such audit.

### 9.4 Conditions of Audit.

- a. Audits conducted pursuant to this Security Attachment must: (i) be conducted during reasonable times and be of reasonable duration; (ii) not unreasonably interfere with DocuSign's day-to-day operations; and (iii) be conducted under mutually agreed upon terms and in accordance with DocuSign's security policies and procedures. DocuSign reserves the right to limit an audit of configuration settings, sensors, monitors, network devices and equipment, files, or other items if DocuSign, in its reasonable discretion, determines that such an audit may compromise the security of DocuSign Signature or the data of other DocuSign customers. Customer's audit rights do not include penetration testing or active vulnerability assessments of the Production Environment or DocuSign Systems within their scope.
- b. In the event that Customer conducts an audit through a third party independent contractor, such independent contractor must enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect DocuSign's confidential information.



- c. Customer must promptly provide DocuSign with any audit, security assessment, compliance assessment reports and associated findings prepared by it or its third party contractors for comment and input prior to formalization and/or sharing such information with a third party.

9.5 Remediation and Response Timeline. If any audit performed pursuant to this Security Attachment reveals or identifies any non-compliance by DocuSign of its obligations under the Agreement and this Security Attachment, then (a) DocuSign will work to correct such issues; and (b) Customer may request feedback and information regarding corrective and remedial actions taken in relation to such audit for no more than 60 days after the date upon which such audit was conducted.

# ATTACHMENT IV

## SERVICE SCHEDULE for DOCUSIGN CLM

Service Schedule revision date: December 11, 2019. Unless otherwise defined in this Service Schedule, capitalized terms will have the meaning given to them in the Agreement.

### 1. DEFINITIONS

“DocuSign CLM” means the on-demand DocuSign Service consisting of enterprise contract management software applications and platform solutions provided via the Internet. This definition shall include, but not be limited to, DocuSign’s enterprise contract management software applications and platform solutions previously called “SpringCM”.

“System” refers to the software systems and programs, the communication and network facilities, and the hardware and equipment used by DocuSign or its agents to make available the DocuSign CLM service via the Internet.

### 2. ADDITIONAL USAGE LIMITATIONS AND CUSTOMER RESPONSIBILITIES

2.1 DocuSign’s provision of DocuSign CLM is conditioned on Customer’s acknowledgement of and agreement to the following:

(a) DocuSign CLM facilitates the generation, management and revision of agreements, forms and other content. Nothing in this Service Schedule may be construed to make DocuSign a party to any such content generated by and/or processed through DocuSign CLM, and DocuSign makes no representation or warranty regarding the Customer Data and/or other content generated, stored and/or shared using DocuSign CLM;

(b) Between DocuSign and Customer, Customer has exclusive control over and responsibility for the quality, format and contents of any Customer Data generated, stored and/or shared using DocuSign CLM. Without limiting the foregoing, DocuSign shall not access Customer Data or other Customer content except to the extent Customer authorizes DocuSign to access the Customer’s Account;

(c) Customer may use DocuSign CLM to send requests for electronic review of specific content or Customer Data generated by and/or stored on the System to third-party users who are not Authorized Users (e.g., Customer’s customers and/or vendors), or to otherwise make Customer Data available to such third-party users through DocuSign CLM. Customer shall be responsible for the activities conducted by its third-party users within DocuSign CLM;

(d) DocuSign is not responsible for determining how long any contracts, documents, and/or other content are required to be retained or stored under any applicable laws, regulations, or legal or administrative agency processes. Further, DocuSign is not responsible for or liable to produce any of Customer’s eDocuments, Customer Data or other documents to any third parties;

(e) Customer agrees that its assigned Account Administrator has authority to provide DocuSign with any required authorizations, requests, or consents on behalf of Customer with respect to Customer's Account; and

(f) Customer agrees it is solely responsible for the accuracy and appropriateness of instructions given by it and its personnel to DocuSign in relation to the DocuSign Services, including without limitation instructions through its Account as made by the assigned Account Administrator.

3. **DOCUMENT STORAGE AND DELETION.** DocuSign shall make Customer Data available to Customer for no less than 90 days following the expiration or termination of this Services Schedule. If Customer fails to retrieve its Customer Data prior to the expiration or termination of the Service Schedule, Customer may request, no later than ninety (90) days after such expiration or termination, that DocuSign provide Professional Services to assist in retrieving Customer Data still remaining on the System, the details of which Professional Services will be set out in a SOW. After such ninety (90) day period, DocuSign shall have no obligation to maintain or provide any Customer Data and DocuSign shall have the right to delete all Customer Data in the System or otherwise in its possession or under its control and delete Customer's Account.

#### 4. INFORMATION SECURITY AND DATA PROCESSING

4.1 **Security.** DocuSign will use commercially reasonable technical and organizational measures designed to prevent unlawful or unauthorized access, use, alteration, or disclosure of Customer Data or other Customer content in accordance with the provisions of DocuSign's Security Attachment for DocuSign CLM attached to this Service Schedule. .

5. **DISCLAIMER.** Except for the express representations and warranties stated in the MSA, and subject to the additional limitations of liability therein, DocuSign: (a) makes no additional representation or warranty of any kind -- whether express, implied in fact or by operation of law, or statutory -- as to any matter whatsoever; (b) disclaims all implied warranties of merchantability and fitness for a particular purpose and the like; and (c) does not warrant that DOCUSIGN CLM is or will be uninterrupted or error-free or meet Customer's requirements. Customer has no right to make or pass on any representation or warranty on behalf of DocuSign to any third party.

# ATTACHMENT V

## SECURITY ATTACHMENT for DOCUSIGN CLM

Service Attachment version date: December 11, 2019.

This Security Attachment for DocuSign CLM (“Security Attachment”) sets forth DocuSign’s commitments for the protection of Customer Data and is made part of the Service Schedule for DocuSign CLM. The terms of this Security Attachment are limited to the scope of the DocuSign CLM service and are not applicable to any other Service Schedules or DocuSign Services. Unless otherwise defined in this Security Attachment, capitalized terms will have the meaning given to them in the Agreement.

### 1. DEFINITIONS

“Personnel” means all employees and agents of DocuSign involved in the performance of the DocuSign CLM service.

“Process” or “Processing” means, with respect to this Security Attachment, any operation or set of operations that is performed upon Customer Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure, or destruction.

“Production Environment” means the System setting where software, hardware, data, processes, and programs are executed for their final and intended operations by end users of DocuSign CLM.

“Subcontractor” means a third party engaged to perform all or a portion of the DocuSign CLM service on behalf of DocuSign or DocuSign’s Affiliates.

### 2. INFORMATION SECURITY PROGRAM

2.1 Information Security Program. DocuSign maintains, and will continue to maintain, a written information security program that includes policies, procedures, and controls governing the Processing of Customer Data through DocuSign CLM (the “Information Security Program”). The Information Security Program is designed to protect the confidentiality, integrity, and availability of Customer Data by using a multi-tiered technical, procedural, and people-related control approach in accordance with industry best practices and applicable laws and regulations, including the Oregon Consumer Information Protection Act, ORS 646A.600 to 646A.628.

2.2 Permitted Use of Customer Data. DocuSign will not Process Customer Data in any manner other than as permitted or required by the Agreement.

2.3 Acknowledgement of Shared Responsibilities. The security of data and information that is accessed, stored, shared, or otherwise processed via a multi-tenant cloud service such as DocuSign CLM are shared responsibilities between a cloud service provider and its customers. As

such, the Parties acknowledge that: (a) DocuSign is responsible for the implementation and operation of the Information Security Program and the protection measures described in this Security Attachment; and (b) Customer is responsible for properly implementing access and use controls and configuring certain features and functionalities of DocuSign CLM that Customer may elect to use DocuSign CLM in the manner that Customer deems adequate to maintain appropriate security, protection, deletion, and backup of Customer Data.

2.4 **Applicability to Customer Data.** This Security Attachment and the Information Security Program apply specifically to the Customer Data Processed via DocuSign CLM. To the extent Customer exchanges data and information with DocuSign that does not meet the definition of "Customer Data," DocuSign will treat such data and information in accordance with the confidentiality terms set forth in the Agreement.

### 3. SECURITY MANAGEMENT

3.1 **Maintenance of Information Security Program.** DocuSign will implement appropriate technical and organizational measures to protect Customer Data located in DocuSign CLM and will maintain the Information Security Program in accordance with standards set forth in NIST Special Publication 800-53, Revision 5, or such other alternative standards that are substantially equivalent to NIST Special Publication 800-53, Revision 5, and other generally recognized industry standards for security, including, but not necessarily limited to, the following (or, as applicable, those issued by the following organizations):

(a) Open Web Application Security Project (OWASP) - see <https://www.owasp.org>;

(b) National Institute for Standards and Technology, including NIST Special Publication 800-53, Revision 5 - see <https://csrc.nist.gov/>;

(c) The State of Oregon 2019 Statewide Information and Cyber Security Standards set forth at: <https://www.oregon.gov/das/OSCIO/Documents/2019StatewideInformationAndCyberSecurityStandardsV1.0.pdf>; and

(d) Data Security Standards (DSS).

DocuSign may update or modify the Information Security Program from time to time provided that such updates and modifications comply with the standards set forth above, and do not result in the degradation of the overall security of DocuSign CLM.

3.2 **Background Checks and Training.** DocuSign will conduct reasonable and appropriate background investigations on all Personnel in accordance with applicable laws and regulations. Personnel must pass DocuSign's background checks prior to being assigned to positions in which they will, or DocuSign reasonably expects them to, have access to Customer Data. DocuSign will conduct annual mandatory security awareness training to inform its Personnel on procedures and policies relevant to the Information Security Program and of the consequences of violating such procedures and policies. DocuSign will conduct an offboarding or exit process with respect to any Personnel upon termination of employment, which will include the removal of the terminated Personnel's access to Customer Data and DocuSign's sensitive systems and assets, including mobile devices.

3.3 Subcontractors. DocuSign will evaluate all Subcontractors to ensure that Subcontractors maintain adequate physical, technical, organizational, and administrative controls, based on the risk tier appropriate to their subcontracted services, that support DocuSign's compliance with the requirements of this Security Attachment. DocuSign requires all Subcontractors to be subject to independent audit assessment as part of, or maintain an independent audit assessment which conforms to, DocuSign's ISO 27001 audit or an equivalent standard, where their roles and activities are reviewed per control requirements. DocuSign will remain responsible for the acts and omissions of its Subcontractors as they relate to the services performed under this Security Attachment as if it had performed the acts or omissions itself and any subcontracting will not reduce DocuSign's obligations to Customer under this Security Attachment.

DocuSign will not transmit, exchange, or otherwise disclose Customer Data or other Customer data to any third parties except in accordance with the Agreement and this Security Attachment. Customer's Account Administrators are responsible for controlling how DocuSign CLM shares information with third parties through configuration of Customer's Account within DocuSign CLM.

3.4 Risk Management Plan. DocuSign shall maintain a documented security risk management plan and will provide Customer a copy of such plan upon request and notify Customer of any changes to the security risk management plan.

3.5 Location of Services and Customer Data. Except with the Customer's express written permission, the DocuSign CLM services (including storage and backup of Customer Data and disaster recovery services and infrastructure), shall be provided solely from within the continental United States and on computing and data storage devices residing therein. In the event DocuSign has secured the Customer's permission to perform some of the DocuSign CLM Services from outside the United States, DocuSign will comply with the Customer's reasonable written security requirements made as conditions of such permission.

3.6 Risk and Security Assurance Framework Contact. Customer's account management team at DocuSign will be Customer's first point of contact for information and support related to the Information Security Program. The DocuSign account management team will work directly with Customer to escalate Customer's questions, issues, and requests to DocuSign's internal teams as necessary.

#### 4. PHYSICAL SECURITY MEASURES

4.1 General. DocuSign will maintain appropriate physical security measures designed to protect the tangible items, such as physical computer systems, networks, servers, and devices, that Process Customer Data. DocuSign will utilize commercial grade security software and hardware to protect the DocuSign CLM service and the Production Environment.

4.2 Corporate Access. DocuSign will ensure that: (a) access to DocuSign's corporate facilities is tightly controlled through, at a minimum, physical access card identification; (b) all visitors to its corporate facilities sign in, agree to confidentiality obligations, and be escorted by Personnel while on premises at all times; and (c) that visitor logs are reviewed by DocuSign's security team on a regular basis. DocuSign will revoke Personnel's physical access to DocuSign's corporate facilities upon termination of employment.

4.3 **Data Center Access.** DocuSign's data centers are included in DocuSign's ISO 27001 or equivalent certification. DocuSign will ensure that its commercial-grade data center service providers used in the provision of DocuSign CLM maintain an on-site security operation that is responsible for all physical data center security functions and formal physical access procedures in accordance with SOC 1 and SOC 2, or equivalent, standards. All data centers that house or store Customer Data will be subject to the following:

(a) Multi-factor physical security measures that have auditable entry/exit mechanisms that record the identity of any individual who enters and leaves the facility must be used.

(b) DocuSign's systems in any such data centers will be stored in locked private cages. Only authorized Personnel will have access to the cages. Third-party vendors and guests must be escorted by authorized Personnel while in the cage.

(c) The following environmental security controls must be in place: (i) uninterruptible power supplies and secondary power supplies on all key systems; (ii) temperature and humidity controls for the heating, ventilation, and air conditioning equipment; (iii) heat and smoke detection devices and fire suppression systems; and (iv) periodic inspection by a fire marshal or similar safety official.

## 5. LOGICAL SECURITY

5.1 **Access Controls.** DocuSign will maintain a formal access control policy and employ a centralized access management system to control Personnel access to the Production Environment.

(a) DocuSign will ensure that all access to the Production Environment is subject to successful two-factor authentication globally from both corporate and remote locations and is restricted to authorized Personnel who demonstrate a legitimate business need for such access. DocuSign will maintain an associated access control process for reviewing and implementing Personnel access requests. DocuSign will regularly review the access rights of authorized Personnel and, upon change in scope of employment necessitating removal or employment termination, remove or modify such access rights as appropriate.

(b) DocuSign will monitor and assess the efficacy of access restrictions applicable to the control of DocuSign's system administrators in the Production Environment, which will entail generating system individual administrator activity information and retaining such information for a period of at least twelve (12) months.

(c) DocuSign will not use Customer Data from the DocuSign CLM service Production Environment in non-production environments without Customer's express permission.

5.2 **Auditing and Logging.** With respect to system auditing and logging, DocuSign will do the following:

(a) DocuSign will use and maintain an auditing and logging mechanism that, at a minimum, captures and records successful and failed user logons and logoffs (with a date and time stamp, user ID, application name, and pass/fail indicator). User access activities will be logged and

audited periodically by DocuSign to identify unauthorized access and to determine possible flaws in DocuSign's access control system.

(b) All application components that have logging capabilities (such as operating systems, databases, web servers, and applications) will be configured to produce a security audit log.

(c) Audit logs will be configured for sufficient log storage capacity.

(d) Each log will be configured so that it cannot be disabled without proper authorization and will send alerts for the success or failure of each auditable event.

(e) Access to security log files will be limited to authorized Personnel, and to Customer upon request.

(f) In regard to DocuSign's development, access to source code by team members must be reviewed at least every ninety (90) days.

(g) In regard to DocuSign's support, DocuSign CLM will maintain a process to help assure that any individual leaving DocuSign's team that provides support to Customer will lose access to Customer's accounts and data upon termination of employment or as soon as reasonably possible after moving to another position within DocuSign.

**5.3 Network Security.** DocuSign will maintain a defense-in-depth approach to hardening the Production Environment against exposure and attack. DocuSign will maintain an isolated Production Environment that includes commercial-grade network management controls such as load balancers, firewalls, intrusion detection systems distributed across production networks, and malware protections. DocuSign will complement its Production Environment architecture with prevention and detection technologies that monitor all activity generated and send risk-based alerts to the relevant security groups.

**5.4 Malicious Code Protection.** DocuSign will ensure that: (a) its information systems and file transfer operations have effective and operational anti-virus software; (b) all anti-virus software is configured for deployment and automatic update; and (c) applicable anti-virus software is integrated with processes and will automatically generate alerts to DocuSign's Cyber Incident Response Team for their investigation and analysis if potentially harmful code is detected.

**5.5 Code Reviews.** DocuSign will maintain a formal software development lifecycle that includes secure coding practices against OWASP and related standards and will perform both manual and automated code reviews. DocuSign's engineering, product development, and product operations management teams will review changes included in production releases to verify that developers have performed automated and manual code reviews designed to minimize associated risks.

**5.6 Vulnerability Scans and Penetration Tests.** DocuSign will perform both internal and external vulnerability scanning and application scanning. Quarterly external scans and annual penetration tests against DocuSign CLM and the Production Environment will be conducted by external qualified, credentialed, and industry-recognized organizations. DocuSign will remedy vulnerabilities identified during scans and penetration tests in a commercially reasonable manner



and timeframe based on severity. Upon Customer's reasonable written request, DocuSign will provide third-party attestations resulting from vulnerability scans and penetration tests per independent external audit reports. For clarification, under no circumstance will Customer be permitted to conduct any vulnerability scans or penetration testing against the Production Environment.

## 6. STORAGE, ENCRYPTION, DISPOSAL AND ACCESS

6.1 **Storage and Separation.** Customer Data will be stored within the physical and logical infrastructure for the DocuSign CLM service at DocuSign's colocation or data center facilities. Exceptions with respect to storage may only be made with Customer's written authorization for specific purposes, such as, for example, extraction of Customer Data for storage on encrypted portable media. DocuSign will logically separate Customer Data located in the Production Environment from other DocuSign customer data.

6.2 **Encryption Technologies.** DocuSign will encrypt Customer Data in accordance with industry best practice standards and as follows:

(a) DocuSign and the DocuSign CLM service will encrypt information in transit using strong encryption techniques and standard security protocols (such as SSL, SSH, IPSEC, SFTP, or secure channel signing and sealing) will be used for transmitting sensitive information (including Customer Data), with configurations that meet PCI standards with regard to data transmitted via the Internet and associated configuration baselines (i.e., ciphers and protocols). Any electronic transmission or exchange of data with DocuSign CLM will be conducted via secure means (using HTTPS, SFTP, or an equivalent protocol), and capabilities to encrypt email transmission will be used when the receiving infrastructure supports such encryption.

(b) DocuSign and the DocuSign CLM service will encrypt information at rest using cryptographic mechanisms to protect the confidentiality and integrity of structured and unstructured data on all servers hosting DocuSign CLM and any Customer Data. AES-256 (or most recent FIPS-approved methods) cryptographic keys will be generated to encrypt information at rest. Databases, object stores, and search indexes will be maintained on encrypted data files, file systems, or self-encrypting drives that use FIPS-approved methods.

(c) DocuSign and the DocuSign CLM service will encrypt information for backup and recovery using a commercially supported encryption solution.

(d) DocuSign and the DocuSign CLM service will conduct encryption key management as follows:

(i) DocuSign shall maintain encryption key management policies, and only a limited group of DocuSign's Personnel will have access to create, distribute, and destroy keys.

(ii) Management and usage of encryption keys for DocuSign CLM will be separate duties.

(iii) All public certificate authorities will meet prevalent industry standards and support all then-current, widely used operating systems.

(iv) Configurations for key strength will conform to the DSS.

(v) Encryption of data at rest for DocuSign CLM will use FIPS 140-2 algorithms and storage standards will conform to NIST 800-111.

(vi) Configurations of encryption protocols, cipher suites, and related settings for encryption of data in transit will conform to DSS.

**6.3 Return or Destruction of Customer Data and Other Customer Assets.** At any time upon the Customer's demand DocuSign will promptly return to the Customer or destroy all Customer Data, files, records, documents, materials, and other items which contain any Data and all other Customer assets in DocuSign's possession or control. Any copies thereof shall also be returned. DocuSign will comply with this requirement with or without a termination of the Agreement. In the absence of such a demand, DocuSign will return or destroy in accordance with Section 6.4 all such Customer Data and other Customer assets upon the termination of the Contract. DocuSign's failure to comply with this subsection shall be a material breach of the Agreement.

**6.4 Disposal.** DocuSign will maintain a data disposal and re-use policy for managing assets and implement industry recognized processes and procedures for equipment management and secure media disposal, which includes erase, destroy, and render unrecoverable all Customer Data within 90 days after any termination of the Agreement. Media will be destroyed and rendered unrecoverable on DocuSign CLM in accordance with the standards identified in the National Institute of Standards' Guidelines for Media Sanitization, SP800-88.

## **7. BUSINESS CONTINUITY AND DISASTER RECOVERY**

**7.1 Continuity Plan.** DocuSign will maintain a written business continuity and disaster recovery plan that addresses the availability of DocuSign CLM ("Continuity Plan"). The Continuity Plan will include elements such as: (a) crisis management, plan and team activation, event and communication process documentation; (b) business recovery, alternative site locations, and call tree testing; and (c) infrastructure, technology, system(s) details, recovery activities, and identification of the Personnel and teams required for such recovery. DocuSign will, at a minimum, conduct a test of the Continuity Plan on an annual basis.

**7.2 DocuSign CLM Continuity.** DocuSign's production architecture for DocuSign CLM is designed to perform secure replication in near real-time to multiple active systems in geographically distributed and physically secure data centers. DocuSign will ensure that: (a) infrastructure systems for DocuSign CLM have been designed to eliminate single points of failure and to minimize the impact of anticipated environmental risks; (b) each data center supporting DocuSign CLM includes full redundancy and fault tolerance infrastructure for electrical, cooling, and network systems; and (c) Production Environment servers are enterprise-scale servers with redundant power to ensure maximum uptime and service availability.

**7.3 DocuSign CLM Disaster Recovery.** In the event of a failure of critical services, DocuSign will restore critical service capability and the production capability of critical information technology infrastructure of DocuSign CLM (including, but not limited to, data centers, hardware, software and power systems, and critical voice, data, and e-commerce communications links). It is DocuSign's responsibility to cause any of its Subcontractors or outsourcers performing activities

that could impact critical processes of DocuSign CLM to have plans in place that meet the same standards as required of DocuSign hereunder. With respect to DocuSign CLM disaster recovery:

(a) DocuSign will promptly respond to Customer's reasonable requests for information regarding DocuSign's Continuity Plan, including, but not limited to, answering emails, returning phone calls, and promptly providing requested updates as to any material revisions of such plans.

(b) Notwithstanding anything to the contrary in the Agreement (including this Security Attachment) and without limiting any of DocuSign's responsibilities thereunder, DocuSign will not be required to provide business continuity or disaster recovery plans for its colocation or data center facilities to Customer. However, publicly available information and references to the capabilities of any such colocation or data center facility will be provided by DocuSign upon request.

(c) DocuSign shall assess and update its Continuity Plan on an annual basis. Such assessments and updates shall consider the nature and extent of the services then being performed by DocuSign in light of then-current business and technology risks. Upon Customer's request (but not more frequently than once in any period of twelve (12) consecutive months), DocuSign shall attest to Customer that it has conducted such an assessment and update of its Continuity Plan.

(d) DocuSign shall conduct comprehensive tests of its Continuity Plan and DocuSign will verify that testing of all critical colocation or data center facility equipment (i.e., power generators and critical IT infrastructure) has been conducted by its colocation or data center facility providers, no less frequently than once in each period of twelve (12) consecutive months. DocuSign's Continuity Plan shall provide for remediation of any deficiencies discovered during any such Continuity Plan testing within timeframes reasonably commensurate with the level of risk posed by the deficiency.

(e) The internal and independent audit reports described in Section 9.1 (Independent Assurances) will evidence or report on the execution of DocuSign's Continuity Plan tests and any resulting remedial actions.

(f) Upon experiencing an applicable material business disruption involving DocuSign CLM, DocuSign will promptly invoke and execute its Continuity Plan and, except as otherwise provided in the applicable Continuity Plan, DocuSign will use commercially reasonable efforts to promptly notify Customer's DocuSign CLM Account Administrators of the issue.

## 8. INCIDENT RESPONSE AND BREACH NOTIFICATION

8.1 **General.** DocuSign will maintain a tested incident response program, which will be managed and run by DocuSign's dedicated Global Incident Response Team. DocuSign's Global Incident Response Team will operate to a mature framework that includes incident management and breach notification policies and associated processes. DocuSign's incident response program will include, at a minimum, initial detection, initial tactical response, initial briefing, incident briefing, refined response, communication and message, formal containment, formal incident report, and post mortem/trend analysis.

**8.2 Breach Notification.** Unless notification is delayed by the actions or demands of a law enforcement agency, DocuSign shall report to Customer any unlawful access or unauthorized acquisition, use, or disclosure of Customer Data persisted in DocuSign CLM (a “Data Breach”) within one calendar day following determination by DocuSign that a Data Breach has occurred. DocuSign’s obligation to report a Data Breach under this Security Attachment is not and will not be construed as an acknowledgement by DocuSign of any fault or liability of DocuSign with respect to such Data Breach.

**8.3 Breach Response.** DocuSign shall take reasonable measures to mitigate the cause of any Data Breach and shall take reasonable corrective measures to prevent future Data Breaches. As information is collected or otherwise becomes available to DocuSign and unless prohibited by law, DocuSign shall provide information regarding the nature and consequences of the Data Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies, and/or credit bureaus. Due to the encryption configuration and security controls associated with DocuSign CLM, DocuSign may not have access to or know the nature of the information contained within Customer’s eDocuments or Customer Data and, as such, the Parties acknowledge that it may not be possible for DocuSign to provide Customer with a description of the type of information or the identity of individuals who may be affected by a Data Breach. Customer is solely responsible for determining whether to notify impacted individuals and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer’s use of DocuSign CLM need to be notified of a Data Breach.

## 9. INDEPENDENT ASSURANCES AND AUDITS

**9.1 Independent Assurances.** DocuSign uses independent external auditors to verify the adequacy of its Information Security Program. Upon Customer’s reasonable written request, DocuSign will provide Customer with third-party attestations, certifications, and reports relevant to the establishment, implementation, and control of the Information Security Program, including DocuSign’s ISO 27001 certification, DSS certification, and Service Organization Controls (SOC) 2, Type 2 reports.

**9.2 Regulatory Audit.** If Customer’s governmental regulators require that Customer perform an on-site audit of DocuSign’s Information Security Program, as supported by evidence provided by Customer, Customer may at Customer’s expense, either through itself or a third-party independent contractor selected by Customer, conduct an on-site audit of DocuSign’s Information Security Program, including DocuSign’s data centers and corporate facilities relevant to the security of Customer Data (“Regulatory Audit”). Customer must submit any requests for an onsite Regulatory Audit to its DocuSign account management representative, who will work with DocuSign’s internal teams to schedule such audit. If a Regulatory Audit requires the equivalent of more than one business day of Personnel’s time to support such audit, DocuSign may, at its discretion, charge Customer an audit fee at DocuSign’s then-current rates, which will be made available to Customer upon request, for each day thereafter.

**9.3 Audit for Data Breach.** Following a Data Breach, DocuSign will, upon Customer’s written request, promptly engage a third-party independent auditor, selected by DocuSign and at DocuSign’s expense, to conduct an on-site audit of DocuSign’s Information Security Program, including DocuSign’s data centers and corporate facilities relevant to the security of Customer Data. DocuSign will promptly provide Customer with the report of such audit.

#### 9.4 Conditions of Audit.

(a) Audits conducted pursuant to this Security Attachment must: (i) be conducted during reasonable times and be of reasonable duration; (ii) not unreasonably interfere with DocuSign's day-to-day operations; and (iii) be conducted under mutually agreed upon terms and in accordance with DocuSign's security policies and procedures. DocuSign reserves the right to limit an audit of configuration settings, sensors, monitors, network devices and equipment, files, or other items if DocuSign, in its reasonable discretion, determines that such an audit may compromise the security of DocuSign CLM or the data of other DocuSign customers. Customer's audit rights do not include penetration testing or active vulnerability assessments of the Production Environment or DocuSign Systems within their scope.

(b) In the event that Customer conducts an audit through a third-party independent contractor, such independent contractor must enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect DocuSign's confidential information.

(c) Customer must promptly provide DocuSign with any audit, security assessment, compliance assessment reports, and associated findings prepared by it or its third-party contractors for comment and input prior to formalization and/or sharing such information with a third party.

9.5 Remediation and Response Timeline. If any audit performed pursuant to this Security Attachment reveals or identifies any non-compliance by DocuSign of its obligations under the Security Attachment, then (a) DocuSign will work to correct such issues; and (b) Customer may request feedback and information regarding corrective and remedial actions taken in relation to such audit for no more than sixty (60) days after the date upon which such audit was conducted.

ATTACHMENT VI  
RESELLER PRICE GUARANTEE



April 7, 2021

Oregon Department of Administrative Services  
155 Cottage St. NE, #U90  
Salem, Oregon 97301

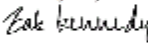
**Subject: DocuSign – State of Oregon Discounting Structure**

To Whom it may concern:

This letter is to confirm that Carahsoft Technology is understanding and in agreement of the discounting structure that has been negotiated directly between DocuSign and the State of Oregon. The State of Oregon will receive a minimum discount of 18% off of list price from Carahsoft and in certain bulk purchasing scenarios may qualify for discounting above and beyond the minimum discount percent.

Please feel free to reach out if any further clarification is needed.

Yours sincerely,

DocuSigned by:  
  
187862822@carahsoft.com

**Zak Kennedy**  
Team Lead  
(703) 230-7430  
[zak.kennedy@carahsoft.com](mailto:zak.kennedy@carahsoft.com)