

DOCUSIGN MASTER SERVICES AGREEMENT

This DocuSign Master Services Agreement (“**MSA**”) is made between DocuSign, Inc., a Delaware corporation (“**DocuSign**”), and the contracting party identified on the Order Form (“**Customer**”), together referred to as the “**Parties**” and each individually as a “**Party**”, as of the date of last signature below (the “**MSA Effective Date**”). The Parties hereby agree to the terms and conditions of this MSA, including any specific services terms, product details and any applicable license and/or subscription terms will be set forth in Attachment A DocuSign Service Schedule, Attachment B CLM Service Schedule, Attachment C Security for DocuSign Services, Attachment D Data Protection for DocuSign Services, Order Form(s) and SOW(s), each of which become binding on the Parties and are incorporated into this MSA upon execution of an Order Form and/or SOW. Each Order Form and/or SOW is governed by and incorporates the following documents in effect as of the effective date of the applicable Order Form or SOW, collectively referred to as the “**Agreement**”, that consists of:

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

The applicable attachment(s), addenda, 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.

MSA Version: September 20, 2021

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 any entity that the Party directly or indirectly owns or controls more than fifty percent (50%) of the voting interests of the subject entity. Any legal entity will be considered a Party’s Affiliate as long as that interest is maintained.

“**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 in Customer’s Account 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 the 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, Documentation and other related technical information, security policies and processes, product roadmaps, and pricing; (b) for Customer and its Affiliates, Customer Data; (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 should reasonably understand it to be confidential information of the disclosing Party; and (d) the terms and conditions of the Agreement between the Parties. Confidential Information does not include any information that: (i) was or becomes generally known to the public through no fault or breach of the 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 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 Cloud 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 Service(s)" means the services provided by DocuSign under an Order Form or SOW, and may include software, source code, or other technology licensed to DocuSign from third parties and embedded into the services that DocuSign provides to Customer. Notwithstanding the foregoing, DocuSign Services do not include Third-Party Services (defined below).

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

"Indemnified Party(ies)" means the Party (whether DocuSign or Customer) being indemnified under Section 9 (Third-Party Claims), 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 provided by DocuSign that sets forth the pricing and 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**").

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

"System" means 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 Services via the Internet.

"Third-Party Services" means services, software, products, applications, integrations and other features or offerings that are provided by Customer or obtained by Customer from a third party.

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 the Agreement, DocuSign grants to Customer a worldwide, limited, non-exclusive, non-transferable right and license during the Term, solely for its and its Affiliates' internal business purposes, and in accordance with the Documentation, to: (a)

access and 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 the Agreement, and Customer is responsible for their acts and omissions relating to the Agreement as though they were those of Customer. A Customer Affiliate may enter into an Order Form or SOW directly with DocuSign under this MSA by a mutually executed Order Form or SOW that references this MSA. In such event: (i) the Customer Affiliate will be bound by this MSA and will be fully responsible for its liabilities and obligations under the applicable Order Form or SOW; and (ii) all references to "**Customer**" in the Agreement will be deemed references to the Customer Affiliate set forth on the Order Form or SOW for purposes of defining the rights and obligations of the Parties hereunder.

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 the 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 the 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, or copy any of the DocuSign Services or technologies, or otherwise attempt to derive source code or other trade secrets or create any derivative works from or about any of the DocuSign Services or technologies, or use the machine-learning algorithm output generated from the DocuSign Services to train, calibrate, or validate, in whole or in part, any other systems, programs or platforms, or for benchmarking, software-development, or other competitive purposes, except pursuant to Customer's non-waivable rights under applicable law, without DocuSign's written 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 avoid interference with or disruption to the integrity, operation, performance, or use or enjoyment by others of the DocuSign Services;
- (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 Services 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 the 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.

2.4 Third-Party Services. Customer may choose to obtain Third-Party Services from third parties and/or DocuSign (for example, through a reseller arrangement or otherwise). Any acquisition by Customer of Third-Party Services is solely between Customer and the applicable Third-Party Service

provider and DocuSign does not warrant, support, or assume any liability or other obligation with respect to such Third-Party Services, unless expressly provided otherwise in the Order Form or the Agreement. In the event Customer chooses to integrate or interoperate Third-Party Services with DocuSign Services in a manner that requires DocuSign or the DocuSign Services to exchange Customer Data with such Third-Party Service or Third-Party Service provider, Customer: (a) grants DocuSign permission to allow the Third-Party Service and Third-Party Service provider to access Customer Data and information about Customer's usage of the Third-Party Services as appropriate and necessary to enable the interoperation of that Third-Party Service with the DocuSign Services; (b) acknowledges that any exchange of data between Customer and any Third-Party Service is solely between Customer and the Third-Party Service provider and is subject to the Third-Party Service provider's terms and conditions governing the use and provision of such Third-Party Service (the presentation and manner of acceptance of which is controlled solely by the Third-Party Service provider); and (c) agrees that DocuSign is not responsible for any disclosure, modification or deletion of Customer Data resulting from access to such data by Third-Party Services and Third-Party Service providers.

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 and 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 (including any machine learning algorithms output from the DocuSign Services) 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 the Agreement.

3.3 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 and its Affiliates 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. Customer shall ensure that: (a) Feedback does not identify Customer, its Affiliates, or Authorized Users, or include any Customer Data; and (b) Customer has obtained requisite authorization from any Authorized User or other third party to grant the license described herein. For the avoidance of doubt, Feedback does not constitute Customer Confidential Information.

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, designed to preserve the security, integrity, and confidentiality of Customer Data and Customer personal data and to protect against unauthorized or unlawful disclosure or corruption of or access to such data in accordance with Attachment C Security Attachment for DocuSign Additional or differing security obligations, if any, will be expressly set forth in the applicable Service Schedule, Order Form, or separate written agreement between the Parties.

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 Data Protection Attachment D for DocuSign Services, for the sole purpose of and

only to the extent necessary for DocuSign, 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 the Agreement.

4.3 Usage Data. DocuSign may collect and use data, information, or insights generated or derived from the use of the DocuSign Services ("**Usage Data**") for its business purposes, including industry analysis, benchmarking, analytics, marketing, and developing, training and improving its products and services. DocuSign will deidentify and anonymize all Usage Data, and will disclose such Usage Data in aggregate form only in a manner that does not identify Customer, its Authorized Users, Customer Data, or Customer's Confidential Information.

5. PAYMENT OF FEES

5.1 Fees. Except as expressly set forth in the applicable Order Form or SOW, Customer will pay all fees set forth in the Order Form or SOW in accordance with the following: (a) DocuSign Services fees are invoiced annually in advance; (b) the first invoice will coincide with the Order Start Date of an Order Form or the effective date of a SOW; (c) payment will be due within thirty (30) days from the date of the invoice; and (d) all amounts will be denominated and payable in the currency specified in the Order Form and/or SOW. Unless otherwise agreed to by the Parties and expressly noted in the Order Form and/or SOW, invoices will be sent to Customer via email. Upon execution by Customer and DocuSign, each Order Form and/or SOW is non-cancellable and non-refundable except as provided in the Agreement, and the Term as set forth in the Order Form for DocuSign Services is a continuous and non-divisible commitment for the full duration of the Term regardless of any invoice schedule. Customer may withhold from payment any charge or amount disputed by Customer in good faith pending resolution of such dispute, provided that Customer: (i) notifies DocuSign of the dispute prior to the date such payment is due, specifying in such notice (A) the amount in dispute, and (B) the reason for the dispute set out in sufficient detail to facilitate investigation by DocuSign and resolution by the Parties; (ii) makes timely payment of all undisputed charges and amounts; (iii) works diligently with DocuSign to resolve the dispute promptly; and (iv) pays all amounts that are determined to be payable by resolution of the dispute (by adversarial proceedings, agreement or otherwise) within ten (10) days following such resolution.

5.2 Purchase Orders. If Customer issues a purchase order, then it shall be for the full amount set forth in the applicable Order Form or SOW, and DocuSign hereby rejects any additional or conflicting terms appearing in a purchase order or any other ordering materials submitted by Customer, and conditions assent solely based on the terms and conditions of the Agreement as offered by DocuSign. Upon request, DocuSign shall reference the purchase order number on its invoices, provided, however, that Customer acknowledges that it is Customer's responsibility to provide the corresponding purchase order information (including a purchase order number) to DocuSign upon the signing of any Order Form. Customer agrees that a failure to provide DocuSign with the corresponding purchase order shall not relieve Customer of its obligations to provide payment to DocuSign pursuant to Section 5.1 (Fees) above.

5.3 Offsets; Late Charges; Attorneys' Fees. If DocuSign owes any amounts to Customer that are not derived from the Agreement, such amounts will not be withheld or offset against any invoice issued under the Agreement. DocuSign may assess late charges equal to the lesser of one and one-half percent (1.5%) of the unpaid balance per month or the highest rate permitted by applicable law. Customer will be responsible for any reasonable attorneys' fees, costs, and expenses incurred by DocuSign to collect any amounts that are not paid when due. If Customer fails to timely pay any amounts due under the Agreement, then without limitation of any of its other rights or remedies, DocuSign may suspend performance of those DocuSign Services until DocuSign receives all past due amounts from Customer.

6. TAXES

6.1 Tax Responsibility. All payments required by the 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**"). Without limiting the foregoing, Customer shall be responsible for and bear Taxes 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, in which case Customer shall increase the amount payable as necessary so that after making all required deductions and withholdings, DocuSign receives and retains (free from any Tax liability) an amount equal to the amount it would have received

had no such deductions or withholdings been made. If Customer claims tax exempt status for amounts due under the 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 the 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 locations set forth on the Order Form or SOW 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 SOW shall expire upon completion of Professional Services or early termination as permitted by the Agreement. The term of this MSA and the Agreement shall continue as long as an Order Form or SOW referencing or incorporated into this MSA remains valid and in effect. Termination or expiration of any Order Form or SOW 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 the Agreement, then the other Party may terminate the 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 the 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 the Agreement expires or is terminated for any reason: (a) Customer will pay to DocuSign any 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 the DocuSign Services and related intellectual property will immediately terminate; (d) DocuSign's obligation to provide any further DocuSign Services to Customer under the Agreement will immediately terminate, except any such DocuSign Services that are expressly to be provided following the expiration or termination of the Agreement; and (e) the Parties' rights and obligations under Sections 4.3, 6.1, 7.3, 8.3, and 10 through 13 will survive.

8. WARRANTIES AND DISCLAIMERS

8.1 DocuSign Service Warranties. DocuSign warrants that: (a) during the applicable Term, the DocuSign Services, when used as authorized under the Agreement, will perform substantially in conformance with the Documentation associated with the applicable DocuSign Services; and (b) DocuSign will use commercially reasonable efforts to ensure that the DocuSign Services do not introduce files, scripts, agents, or programs intended to do harm, including, for example, viruses, worms, time bombs, and Trojan horses into Customer's system. Customer's sole and exclusive remedy for any breach of these warranties 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 the Agreement.

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

8.3 DISCLAIMER. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN THE AGREEMENT, DOCUSIGN: (A) MAKES NO 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 defend and, in accordance with Section 9.3 (Procedures), indemnify Customer's Indemnified Parties from and against, any: (a) third-party claim; (b) third-party legal action; or (c) administrative agency action or proceeding (each, a "**Claim**") to the extent arising from: (i) any actual breach by DocuSign of specified security safeguards under the Agreement 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 right occurring from Customer's use of the DocuSign Services as authorized under the Agreement. Notwithstanding the foregoing, DocuSign will not be responsible for any Claim due to Customer's or its Authorized User's combination of DocuSign Services with goods or services provided by third parties, including any Third-Party Services; adherence to specifications, designs, or instructions furnished by Customer; or Customer's modification of the DocuSign Services not described in the Documentation or otherwise expressly authorized by DocuSign in writing.

9.2 By Customer. Customer will defend and, in accordance with Section 9.3 (Procedures), indemnify DocuSign's Indemnified Parties from and against, any Claim to the extent arising from: (a) use of the DocuSign Services by Customer or its Authorized Users in violation of the Agreement, the Documentation, or applicable law; (b) any breach by Customer of its obligations under Section 2.2 (e) through (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 obligations in this Section 9 (Third-Party Claims) 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) the Indemnifying Party being given full and complete control over the defense and settlement of the Claim; and (c) the relevant Indemnified Parties providing assistance in connection with the defense and settlement of the Claim, as the Indemnifying Party may reasonably request. 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. The Indemnifying Party shall not, without the relevant applicable Indemnified Parties' prior written consent, agree to any settlement on behalf of such Indemnified Parties which includes either the obligation to pay any amounts, or any admissions of liability, whether civil or criminal, on the part of any of the Indemnified Parties.

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 affected portions of the DocuSign Services; (b) modify the allegedly infringing portions of the DocuSign Services so as to avoid the Claim without substantially diminishing or impairing their functionality; or (c) replace the allegedly infringing portions of the DocuSign Services with items of substantially similar functionality so as to avoid the Claim. If DocuSign determines that the foregoing remedies are not commercially reasonable and notifies Customer of such determination, then either Party may terminate the Agreement, and in such case, DocuSign will provide a prorated refund to Customer for any prepaid fees for the infringing DocuSign Services received by DocuSign under the Agreement that correspond to the unused portion of the Term. The remedies set out

in this Section 9 (Third-Party Claims) are Customer's sole and exclusive remedies for any actual or alleged infringement by the DocuSign Services of any third-party intellectual property right.

10. LIMITATION OF LIABILITY

10.1 Exclusion of Damages. EXCEPT FOR THE PARTIES' EXPRESS 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, INDIRECT, SPECIAL, COVER, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE AGREEMENT, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH LOSSES.

10.2 Limitation of Liability. EXCEPT FOR: (A) THE PARTIES' EXPRESS OBLIGATIONS UNDER SECTION 9 (THIRD-PARTY CLAIMS); (B) DAMAGES RESULTING FROM DEATH OR BODILY INJURY, OR PHYSICAL DAMAGE TO TANGIBLE REAL OR PERSONAL PROPERTY, CAUSED BY EITHER PARTY'S NEGLIGENCE; (C) DAMAGES RESULTING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; AND (D) DOCUSIGN'S RIGHT TO COLLECT UNPAID FEES DUE HEREUNDER, TO THE EXTENT PERMITTED BY LAW, THE TOTAL, CUMULATIVE LIABILITY OF EACH PARTY (AND THEIR RESPECTIVE AFFILIATES) ARISING OUT OF OR RELATED TO THE AGREEMENT WILL BE LIMITED TO THE AMOUNTS PAID BY CUSTOMER FOR THE DOCUSIGN SERVICE(S) DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR ANY OTHER LEGAL OR EQUITABLE THEORY. 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 the 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 the Agreement, and each of these provisions will apply even if the warranties in the 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 disclosing 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 disclosing Party, Recipient will give prompt written notice to the disclosing Party before making the disclosure, unless prohibited from doing so by 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 the 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 the 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).

12. GOVERNING LAW AND VENUE

12.1

The Agreement is governed by the laws of the State of Michigan, U.S.A., without reference to its choice of law rules to the contrary. The Parties hereby irrevocably consent to the exclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in Washtenaw County, Michigan, for the purposes of adjudicating any dispute arising out of the Agreement. To the extent permitted by law, choice of law rules, the 1980 U.N. Convention on Contracts for the International Sale of Goods, and the Uniform Computer Information Transactions Act as enacted, shall not apply. Notwithstanding the foregoing, either Party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such Party's intellectual property rights. Each Party hereby irrevocably waives, to the fullest extent permitted by law, any and all right to trial by jury in any legal proceeding arising out of or relating to the Agreement.

12.2 To the extent allowed by law, the English version of the Agreement is binding, and other translations are for convenience only.

13. GENERAL

13.1 Relationship. The Parties are independent contractors. The Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the Parties. Except as set forth in the Agreement, nothing in the 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 the Agreement without the other Party's prior written consent. Notwithstanding the foregoing, either Party may assign its rights and obligations under the 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 the Agreement will be void.

13.3 Notices. Any notice required or permitted to be given in accordance with the 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. 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 the 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. Delays in fulfilling

the obligations to pay hereunder are excused only to the extent that payments are entirely prevented by the Force Majeure Event.

13.5 Trade Restrictions. The DocuSign Services, Documentation, and the provision and any 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 performance of the Agreement. For the avoidance of doubt, nothing in this Agreement is intended to induce or require either Party to act in any manner which is penalized or prohibited under any applicable laws, rules, regulations or decrees.

(b) Customer represents that it is not a Restricted Party. "**Restricted Party**" means any person or entity that is: (i) located or organized in a country or territory subject to comprehensive U.S. sanctions (currently including Cuba, Crimea, Iran, North Korea, Syria) ("**Sanctioned Territory**"); (ii) owned or controlled by or acting on behalf of the government of a Sanctioned Territory; (iii) an entity organized in or a resident of a Sanctioned Territory; (iv) identified on any list of restricted parties targeted under U.S., EU or multilateral sanctions, including, but not limited to, the U.S. Department of the Treasury, Office of Foreign Assets Control's ("**OFAC**") List of Specially Designated Nationals and Other Blocked Persons, the OFAC Sectoral Sanctions List, the U.S. State Department's Nonproliferation Sanctions and other lists, the U.S. Commerce Department's Entity List or Denied Persons List located on the Website of the International Trade Administration, where you will find the consolidated list of persons, groups and entities subject to EU financial sanctions from time to time; or (v) owned or controlled by, or acting on behalf of, any of the foregoing. (c) 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 any Sanctioned Territory.

13.6 Anti-Corruption. In connection with the DocuSign Services performed under the Agreement and Customer's use of the DocuSign 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 Services, including Documentation, and any software as may be provided under an applicable Service Schedule, are deemed to be "commercial computer software" and "commercial computer software documentation". "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 the 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 the 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 Services unless the prior written consent of the other Party has been obtained, provided, however, that DocuSign may use Customer's name and logo for the limited purpose of identifying Customer as a customer of the DocuSign Services.

13.9 Waiver. The waiver by either Party of any breach of any provision of the 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 the 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 the Agreement.

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

13.11 Entire Agreement. The Agreement is the final, complete, and exclusive expression of the agreement between the Parties regarding the DocuSign Services provided under the Agreement. The 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 the 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. The Agreement may be changed only by a written agreement signed by an authorized agent of both Parties. The 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.

The below signatories are authorized to sign on behalf of their respective Party(ies) and to agree to the terms of this MSA and any documents incorporated herein as of the MSA Effective Date.

Customer

DocuSign, Inc.

Signature:

Signature:

Name: William C. Brand

Name:

Title: Mayor

Title:

Date:

Date:

ATTEST:

Eleanor Manzano, City Clerk

APPROVED AS TO FORM:

Michael W. Webb, City Attorney

ADDENDUM to the DocuSign MSA for U.S. PUBLIC ENTITIES

This Addendum to the DocuSign MSA for U.S. Public Entities (“**Addendum**”) is made part of the Master Services Agreement between the Parties. Unless otherwise defined in this Addendum, capitalized terms will have the meaning given to them in the Agreement. This Addendum applies to Customer only if Customer is (i) a United States state or local government or agency thereof, or (ii) a United States public school (including both K-12 and university institutions), but only to the extent the DocuSign Services are being used in an Authorized User’s official capacity as a state, local government, or school official or employee (“**Official Use**”). If there is any conflict between the Addendum and the Agreement, the applicable terms of this Addendum will prevail. Nothing in this Addendum makes DocuSign a government contractor for any federal, state, local, or foreign government.

1. Licensed Use. The phrase “internal business purposes” as used in the Agreement means Official Use by Authorized Users for Customer’s internal purposes.

2. Terms Prohibited by Law. Provisions of the Agreement that cannot be accepted by Customer under Customer’s state constitution or laws shall not apply to the extent of such prohibitions, but will apply to the full extent, if any, permitted by applicable law.

3. Public Records. The provisions of the Agreement regarding Customer’s use of DocuSign Confidential Information are hereby modified to be consistent with Customer’s state law with respect to use and disclosure of public records including without limitation any applicable “Freedom of Information” laws. If Customer is required by law to disclose any information that would be considered to Confidential Information under DocuSign’s standard terms, Customer agrees to make reasonable efforts to notify DocuSign of such disclosure, to limit such disclosure to only that information that is required to be disclosed by law by redacting or withholding information where possible, and to cooperate in any effort reasonably made by DocuSign to prevent or limit such disclosure.

4. Governing Law and Venue. Provisions of the Agreement pertaining to governing law and venue do not apply to Official Use of the DocuSign Services to the extent such provisions are prohibited by Customer’s state constitution or laws, in which case this Agreement is governed by the laws of Customer’s state.

5. No Endorsement. DocuSign agrees that Customer’s seals, trademarks, logos, service marks, trade names, and the fact that Customer has a presence on one of DocuSign’s websites or uses the DocuSign Services, will not be used by DocuSign in such a manner as to state or imply that DocuSign’s products or services are endorsed, sponsored or recommended by Customer or are considered by Customer to be superior to any other products or services without prior approval from Customer or by other relevant government authority. Except for pages whose design and content is under the control of the Customer, or for links to or promotion of such pages, DocuSign agrees not to display any Customer or government seals, trademarks, logos, service marks, and trade names on our homepage or elsewhere on one of DocuSign’s hosted sites unless permission to do so has been granted by Customer or by other relevant government authority. Notwithstanding the foregoing, Customer hereby agrees that DocuSign may list Customer’s name in a publicly available customer list on a DocuSign website or elsewhere so long as the name is not displayed in a more prominent fashion than that of any other third-party customer name.

6. Discrimination and Non-Segregation. DocuSign, Inc. is a federal contractor. As a result, the Equal Opportunity Clause set forth in 41 C.F.R. parts 60-1.4(a), and the employee notice found at 29 C.F.R. Part 471, Appendix A to Subpart A are incorporated by reference herein. In addition, DocuSign shall abide by the requirements of 41 C.F.R. §§ 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals on the basis of protected veteran status or disability, and require affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified protected veterans and individuals with disabilities.

7. FERPA. If Customer wants its students to use the DocuSign Services (permitted only for students age 13 and older), Customer is responsible for complying with the U.S. Family Educational Rights and Privacy Act (“**FERPA**”). This means Customer must notify those students’ parents/guardians of the personally identifiable information that it will collect and share with DocuSign and obtain parental/guardian consent before its students sign up or use the DocuSign Services. When obtaining such consent, Customer should provide parents/guardians with a copy of DocuSign’s Privacy Policy (available upon request). Customer must keep all consents on file and provide them to DocuSign at DocuSign’s reasonable request. If Customer is located outside of the United States, DocuSign will rely upon Customer to obtain any required consents or approvals from the parent or guardian of any student covered

by similar laws and, as a condition to Customer's and its students' use of the DocuSign Services, Customer will comply with such laws. DocuSign acknowledges that, as between DocuSign and Customer, DocuSign may be considered a "School Official" as that term is used in FERPA and its implementing regulations. As such, DocuSign agrees that it will hold all Customer Data (including personal data therein) in strict confidence pursuant to the terms of the Agreement and will not use or disclose Customer Data except: (a) as required to provide the DocuSign Services to Customer or (b) as required by law, but only to the extent permitted and only in the manner prescribed by the law, and (c) as otherwise expressly authorized by the Agreement and in accordance with DocuSign's Privacy Policy (available upon request). This section will not create any obligations on the part of DocuSign outside those set forth in this Agreement.

8. Gramm-Leach-Bliley Act. DocuSign agrees and warrants it has implemented information security policies and safeguards to preserve the security, integrity, and confidentiality of eDocument and to protect against unauthorized access and anticipated threats or hazards thereto, that meet the objectives of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information as set forth in Section 501(b) of the Gramm-Leach-Bliley Act.

Attachment A: 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, 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 the Security Attachment for DocuSign Services found at: <https://www.docusign.com/company/terms-and-conditions/security-attachment-docusign-services>.

4.2 Data Storage/Transfer. If Customer or Customer Affiliate is established in the United Kingdom, a Member State of the European Economic Area, or Switzerland, the Data Protection Attachment for DocuSign Services found at:

<https://www.docusign.com/company/terms-and-conditions/data-protection-attachment>, applies to the processing of any personal data (as defined the General Data Protection Regulation).

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.

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 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 B: SERVICE SCHEDULE for DOCUSIGN CLM

Service Schedule revision date: November 19, 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. 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 the Security Attachment for DocuSign Services.

4.2 Data Storage/Transfer. If Customer or Customer Affiliate is established in the United Kingdom, a Member State of the European Economic Area, or Switzerland, the Data Protection Attachment for DocuSign Services will apply to the processing of any personal data (as defined in the General Data Protection Regulation).

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.

This Security Attachment for DocuSign Services (“Security Attachment”) sets forth DocuSign’s commitments for the protection of Customer Data and is made part of Agreement. 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 engaged in the performance of DocuSign Services to Customer.

“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,

“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 Services.

“Subcontractor” means a third party that DocuSign has engaged to perform all or a portion of DocuSign Services 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 Services (“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.

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 the DocuSign Services are shared responsibilities between DocuSign and Customer. 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. Customer is responsible for properly implementing access and use controls and configuring certain features and functionalities of DocuSign Services that Customer may elect to use DocuSign Services 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 Services and does not extend to data held on Customer’s systems or environments or to any on-premise solutions that may be offered by

DocuSign. 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 Services and will maintain the Information Security Program in accordance with ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001. DocuSign may update or modify the Information Security Program from time to time provided that such updates and modifications do not result in the degradation of the overall security of DocuSign Services.

3.2 Background Checks and Training. DocuSign will ensure that reasonable and appropriate background investigations are conducted on all Personnel in accordance with applicable laws and regulations. Personnel must pass DocuSign's background check requirements 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.

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. 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 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 ensure that commercial grade security software and hardware are utilized to protect DocuSign Services and the Production Environment.

4.2 Facility 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) 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 Centers. DocuSign will use commercial-grade data center service providers in providing the DocuSign Services and will ensure that all data centers conform to ISO 27001 or equivalent certification. At minimum, all data centers must meet the following requirements:

- (a) Multi-factor physical security measures, including auditable entry/exit mechanisms that record the identity of any individual who enters and leaves the facility must be maintained.
- (b) Access must be limited to authorized personnel. Third-party vendors and guests must be escorted at all times by authorized personnel while in the data center.
- (c) Environmental security controls must be in place, including: (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 inspections 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 Production Environment in non-production environments without Customer's express permission.

5.2 Auditing and Logging. With respect to system auditing and logging in the Production Environment:

- (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.

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 if potentially harmful code is detected for their investigation and analysis.

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. 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.

5.6 Vulnerability Scans and Penetration Tests. DocuSign will perform both internal and external vulnerability scanning and application scanning. External scans and penetration tests against DocuSign Services and the Production Environment will be conducted by external qualified, credentialed, and industry recognized organizations on a frequency based on risk but, at a minimum, on an annual basis. DocuSign will remedy vulnerabilities identified during scans and penetration tests in a commercially reasonable manner and timeframe based upon classified and prioritized severity level. DocuSign will make available all 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, AND DISPOSAL

6.1 Storage & Separation. Customer Data will be stored within the physical and logical infrastructure for the DocuSign Services 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 the Documentation, using industry accepted standards, strong encryption techniques, and current security protocols. Electronic transmission or exchange of Customer Data with DocuSign Services will be conducted via secure means.

6.3 Disposal. DocuSign will implement industry recognized processes and procedures for equipment management and secure media disposal under the guidelines 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 written business continuity and disaster recovery plans that address the availability of DocuSign Services ("Continuity Plans"). The Continuity Plans 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. DocuSign's Continuity Plans 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. 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's tests and any resulting remedial actions.

7.2 DocuSign Service Continuity. DocuSign's production architecture for DocuSign Services 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 Services have been designed to eliminate single points of failure and to minimize the impact of anticipated environmental risks; (b) each data center supporting DocuSign Services 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 Disaster Recovery. In the event of a failure of critical services or material business disruption, DocuSign will promptly invoke its Continuity Plans and will restore critical service capability and the production capability of critical information technology infrastructure of the DocuSign Services (including, but not limited to, data centers, hardware, software and power systems, and critical voice, data, and e-commerce communications links), and, except as otherwise provided in the applicable Continuity Plan, DocuSign will use commercially reasonable efforts to promptly notify Customer's Account Administrators of the issue. It is DocuSign's responsibility to cause any of its Subcontractors or outsourcers performing activities that could impact critical processes of DocuSign Services to have plans in place that meet the same standards as required of DocuSign hereunder. 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.

8. DATA INCIDENT RESPONSE AND 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 postmortem/trend analysis.

8.2 Data Incident Notification. DocuSign will comply with all applicable security breach notification laws and regulations in its provision of the DocuSign Services and, in any event, will notify Customer without undue delay upon becoming aware of any breach of DocuSign's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data on systems managed by DocuSign (a "Data Incident"). Without limiting the generality of the foregoing, the Parties acknowledge and agree that Data Incidents do not include unsuccessful attempts, everyday security alerts, or other events that do not materially compromise the security or availability of Customer Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. DocuSign's notification of a Data Incident under this section is not an acknowledgement by DocuSign of any fault or liability with respect to the Data Incident.

8.3 Data Incident Response. DocuSign shall take reasonable measures to mitigate the cause of any Data Incident and shall take reasonable corrective measures to prevent the same Data Incident from occurring in the future. 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 Incident 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 Services, DocuSign may not have access to or know the nature of the information contained within 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 Incident. 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 Services need to be notified of a Data Incident.

9. INDEPENDENT ASSURANCES AND AUDITS

9.1 Independent Assurances. DocuSign uses independent external auditors to verify the adequacy of its Information Security Program. DocuSign will provide or make available to Customer third-party Any audit report includes confidential information and should only be used for the purpose for which it was prepared, i.e. the audit of DocuSign Services. Particularly, because the DocuSign Services are a shared, multi-tenant environment, confidential information such as audit reports should be treated with utmost care and not used for any other purpose other than those described herein attestations, certifications, and reports relevant to the establishment, implementation, and control of the Information Security Program, including, where applicable, ISO 27001 certifications, PCI DSS certifications, and Service Organization Controls (SOC) reports.

9.2 Additional Requirements. To the extent Customer requires additional audit information or assistance from DocuSign beyond those set forth in Section 9.1 (Independent Assurances) as required under applicable laws and regulations, Customer may submit its request for such additional information and assistance, which shall include information regarding the applicable laws or regulations forming the basis of the request, to its account management representative. DocuSign will work with Customer to reach mutually agreed upon terms regarding the scope, timing, duration, and other details regarding such additionally requested information and assistance.

9.3 Audit for Data Incident. Following a Data Incident, DocuSign will within a reasonable timeframe, 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. Upon request, DocuSign will provide or make available a report of such audit to Customer.

9.4 Conditions of Audit.

(a) Any 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 Services 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 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) for no more than sixty (60) days after the date upon which such audit was conducted, Customer may request feedback and information regarding corrective and remedial actions taken in relation to such audit.

This Data Protection Attachment for DocuSign Services ("DPA") is incorporated into and made part of the Agreement. Unless otherwise defined in this DPA, capitalized terms will have the meaning given to them in the Agreement. In the event of any conflict between these documents, the following order of precedence applies (in descending order): (a) Binding Corporate Rules, (b) the alternative data transfer mechanism provided for under Section 6.2 of this DPA; (c) the body of the DPA; (d) any documents attached to the DPA; and (e) the Agreement.

1. DEFINITIONS

"Applicable Data Protection Laws" means all data privacy or data protection laws or regulations that apply to the Processing of Personal Data under the Agreement.

"Binding Corporate Rules" means DocuSign's Binding Corporate Rules for Processors.

"Controller" and "Processor" (or equivalent terms) have the meanings set forth under Applicable Data Protection Laws.

"Data Incident" has the meaning as defined in the Security Attachment for DocuSign Services.

"Data Subjects" has the same meaning as the term "data subject" or equivalent term under Applicable Data Protection Laws.

"DocuSign Service Subprocessor" means a third party, other than the DocuSign contracting entity, which may Process Personal Data on behalf of the DocuSign contracting entity as part of the provision of the DocuSign Services.

"Personal Data" means such "personal data", "personally identifiable information (PII)" or equivalent term under Applicable Data Protection Laws.

"Process/Processing" has the meaning set forth under Applicable Data Protection Laws and includes any operation or set of operations that is performed on Personal 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.

"Regulators" has the same meaning as the term "supervisory authority", "data protection authority" or equivalent term under Applicable Data Protection Laws.

2. GENERAL

2.1 This DPA applies to DocuSign's Processing of Personal Data on Customer's or Customer Affiliate's behalf (as applicable) for the provision of the DocuSign Services as specified in the Agreement. Unless

otherwise expressly stated in the Agreement, this DPA is in effect and remains in force for the Term of the Agreement.

3. PROCESSING RESPONSIBILITY AND CUSTOMER'S INSTRUCTIONS

3.1 Customer is a Controller and DocuSign is a Processor for the Processing of Personal Data with respect to the DocuSign Services provided under the Agreement. Each Party is responsible for compliance with its own respective obligations under Applicable Data Protection Laws. For the avoidance of doubt, DocuSign is not responsible for complying with data protection laws applicable to Customer or Customer's industry such as those not generally applicable to online service providers. Customer acknowledges and agrees that it has met all legal requirements necessary for DocuSign and/or the DocuSign Service Subprocessors to process Personal Data as authorized in the Agreement.

3.2 DocuSign will Process Personal Data only as necessary to provide the DocuSign Services in accordance with the terms of the Agreement or as instructed by Customer in writing, including in electronic form. Subject to Customer's instructions being in accordance with Applicable Data Protection Laws, DocuSign will comply with such instructions to the extent and within such timeframes reasonably necessary for DocuSign to (a) comply with its Processor obligations under Applicable Data Protection Laws; or (b) assist Customer to comply with Customer's obligations under Applicable Data Protection Laws relevant to Customer's use of the DocuSign Services. DocuSign will follow such Customer's instructions at no additional cost to Customer if DocuSign does not expect to incur additional charges or fees not reasonably covered by the fees for the DocuSign Services payable under the Agreement, including, without limitation, additional license or third-party contractor fees. If additional charges or fees are expected, DocuSign will promptly inform Customer upon receiving Customer's instructions and the Parties will negotiate in good faith with respect to any such charges or fees. To the extent required by the Applicable Data Protection Laws, DocuSign will promptly inform Customer if, in DocuSign's opinion, Customer's instruction infringes Applicable Data Protection Laws. Customer acknowledges and agrees that DocuSign is not responsible for performing legal research and/or for providing legal advice to Customer.

3.3 Unless otherwise specified in the Agreement, Customer agrees it will not provide DocuSign with any sensitive or special categories of Personal Data that imposes specific data security or data protection obligations on DocuSign in addition to or different from those specified in this DPA (including any appendix to the DPA) or Agreement.

3.5 With respect to DocuSign's Processing of Personal Data of California Consumers under the California Consumer Privacy Act of 2018 ("CCPA"), the Parties agree that DocuSign acts as a CCPA service provider for Personal Data. Customer acknowledges that it is not selling Personal Data to DocuSign and DocuSign agrees that it will only use Personal Data for the purposes specified in this DPA and the Agreement. Additionally, each Party agrees it will take commercially reasonable steps to avoid any action under the Agreement that would cause the other Party to be deemed to have sold Personal Data under the CCPA.

4. PRIVACY INQUIRIES AND REQUESTS FROM DATA SUBJECTS

4.1 If Customer receives a request or inquiry from a Data Subject related to Personal Data Processed by DocuSign, Customer can either (a) access its DocuSign Services containing Personal Data to address the request or inquiry, or (b) to the extent such access is not available to Customer, contact DocuSign customer support for additional assistance to enable Customer to address the request or inquiry.

4.2 If DocuSign directly receives any requests or inquiries from a Data Subject, DocuSign will promptly pass on such request to Customer if the Data Subject has identified Customer as Controller of the Personal Data forming the base of the request or inquiry. DocuSign may advise the Data Subject to identify and contact the relevant Controller(s) which have uploaded or submitted the Data Subject's Personal Data for Processing by the DocuSign Services. Notwithstanding the foregoing, Customer understands and agrees that as a Controller, Customer is solely responsible for responding to such Data Subject's requests or inquiries and that DocuSign has no responsibility to respond to a Data Subject for or on the Customer's behalf. Regarding any anonymized data or other data not considered Personal Data under Applicable Data Protection Laws, the Parties agree and acknowledge that DocuSign has no obligation as a Processor or under this DPA to re-identify or link information or take any other action which may result in such data being deemed Personal Data.

5. DOCUSIGN AFFILIATES AND THIRD-PARTY SUBPROCESSORS

5.1 Subject to the terms of this DPA and the Agreement, Customer acknowledges and agrees that DocuSign may engage DocuSign Service Subprocessors to Process Personal Data for or on behalf of DocuSign to provide the DocuSign Services. DocuSign will be liable for the performance of all its obligations under the Agreement whether or not it has delegated or subcontracted any of them to a DocuSign Service Subprocessor.

5.2 DocuSign Service Subprocessors are authorized by DocuSign to process Personal Data only in accordance with the terms of this DPA and the Agreement and are subject to the Binding Corporate Rules or bound by written terms at least as protective of Customer's Personal Data as set forth in this DPA. A list of DocuSign's DocuSign Service Subprocessors (including the name and location of such DocuSign Service Subprocessors and the activities it will perform) is available on DocuSign's website at <https://www.docusign.com/trust/privacy/subprocessors-list> (the "Subprocessor List"), and notice regarding new DocuSign Service Subprocessors is made available through a subscription mechanism as described on the DocuSign website. Customer agrees to subscribe to the Subprocessor List in order for DocuSign to notify Customer of new DocuSign Service Subprocessor(s) for the applicable DocuSign Services.

5.3 Customer may object to DocuSign's use of a new DocuSign Service Subprocessor to Process Customer's Personal Data by giving written notice to DocuSign within thirty (30) days of being informed by DocuSign of such a new DocuSign Service Subprocessor. If Customer objects to the use of a new DocuSign Service Subprocessor in compliance with the foregoing, DocuSign has the right to cure the objection within thirty (30) days of DocuSign's receipt of Customer's objection through either of the following options (to be selected at DocuSign's sole discretion): (a) DocuSign providing a commercially reasonable alternative to avoid the Processing of Personal Data by the objected DocuSign Service Subprocessor; or (b) DocuSign terminating the affected DocuSign Services involving use of the new DocuSign Service Subprocessor to Process Customer's Personal Data and providing a prorated refund to Customer for any prepaid fees received by DocuSign under the Agreement corresponding to the unused portion of the Term of such terminated DocuSign Services following the effective date of termination, which is Customer's sole and exclusive remedy for the terminated DocuSign Services.

5.4 If and to the extent the Processing of Personal Data by DocuSign involves a cross-border transfer of Personal Data to any DocuSign Service Subprocessor(s) in a country not recognized as providing an adequate level of protection for Personal Data, the Parties agree that prior to any such transfers taking

place, DocuSign will implement with such DocuSign Service Subprocessor(s) appropriate cross-border transfer safeguards in accordance with the Applicable Data Protection Laws.

6. CROSS-BORDER DATA TRANSFERS

6.1 DocuSign may Process Personal Data globally as necessary to perform the DocuSign Services. To the extent such global access involves a transfer of Personal Data subject to cross-border transfer obligations under Applicable Data Protection Laws within the DocuSign group, the Binding Corporate Rules apply to the Processing of Personal Data by DocuSign and/or its Affiliates as part of the provision of DocuSign Services under the Agreement. The Binding Corporate Rules are incorporated by reference into this DPA, and DocuSign agrees to use commercially reasonable efforts to maintain the regulatory authorization of the Binding Corporate Rules or other appropriate cross-border transfer safeguards for the duration of the Agreement. If Customer has subscribed to be informed of changes to the Binding Corporate Rules through the subscription mechanism described on the DocuSign Alerts page of the DocuSign website, DocuSign will inform Customer of any subsequent material changes to its Binding Corporate Rules through the applicable subscription alerts.

6.2 In the event that the Binding Corporate Rules (including the protections provided therein) together with necessary supplemental measures are deemed inadequate by Regulators for cross-border transfers of Personal Data under Applicable Data Protection Laws, the Parties shall enter into the standard contractual clauses as approved by the European Commission.

7. INFORMATION AND ASSISTANCE

7.1 Upon prior written request, DocuSign will provide to Customer reasonable assistance and information regarding the DocuSign Services provided under the Agreement to assist Customer in (a) Customer conducting a privacy impact assessment of the DocuSign Services, and (b) an investigation by any Regulator(s) to the extent that such investigation relates to Customer's use of the DocuSign Services and Personal Data Processed by DocuSign in accordance with the Agreement.

8. SECURITY SAFEGUARDS

8.1 DocuSign will safeguard Personal Data with appropriate technical, physical, and organizational measures designed to prevent Data Incidents. Additional details regarding the specific security measures that apply to the DocuSign Services are as described in the Binding Corporate Rules and the Agreement. All DocuSign employees, as well as any DocuSign Service Subprocessors that Process Personal Data, are subject to appropriate written confidentiality obligations, including training on information protection, and compliance with DocuSign policies concerning protection of Confidential Information.

8.2 Customer shall be responsible for properly implementing access and use controls and configuring certain features and functionalities of the DocuSign Services that Customer may elect to use and agrees that it will do so in accordance with this DPA and the Agreement in such manner that Customer deems adequate, including, without limitation, maintaining appropriate security, protection, deletion, and backup of its own Personal Data.

9. AUDIT RIGHTS

9.1 The Binding Corporate Rules and Agreement set forth Customer's audit rights as permitted under this DPA. Upon completion of any audit, Customer will provide DocuSign with a copy of the audit report or other summary ("Audit Report"), which is subject to the confidentiality terms of the Agreement. Customer may use the Audit Report only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

9.2 Unless otherwise set forth in the Agreement, each Party will bear its own costs in relation to audits, unless DocuSign promptly informs Customer upon reviewing Customer's audit request that it expects to incur additional charges or fees in the performance of such audit that are not covered by the fees payable under the Agreement, including without limitation additional license or third-party contractor fees. The Parties will negotiate in good faith with respect to any such charges or fees.

9.3 Without prejudice to the rights set forth in Section 9.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third-party auditor within the prior twelve months and DocuSign provides such report to Customer confirming there are no known material changes in the controls audited, Customer agrees to accept the findings presented in the third-party audit report in lieu of requesting an audit of the same or materially similar controls covered by the report.

10. INCIDENT NOTIFICATION AND MANAGEMENT

10.1 DocuSign has implemented controls and policies designed to detect and promptly respond to Data Incidents. DocuSign shall, without undue delay, report to Customer any Data Incident upon becoming aware that a Data Incident has occurred, to the extent not otherwise prohibited under applicable law. DocuSign's obligation to report a Data Incident under this DPA is not and will not be construed as an acknowledgement by DocuSign of any fault or liability of DocuSign with respect to such Data Incident. Customer is solely responsible for determining whether to notify impacted Data Subjects and for providing such notice, and for determining whether Regulators need to be notified of a Data Incident as may be required for Customer's own business and activities. DocuSign shall promptly provide Customer information reasonably requested to support customer's responsibility to notify pursuant to the foregoing, to the extent Customer is not able to obtain such information directly through the features and functionality provided by the DocuSign Services. Notwithstanding the foregoing, Customer agrees to coordinate with DocuSign on the content of Customer's intended public statements or required notices for affected Data Subjects and/or notices to relevant Regulators regarding the Data Incident.

10.2 DocuSign will promptly define escalation paths to investigate such incidents in order to confirm if a Data Incident has occurred, and to take reasonable measures designed to identify the root cause(s) of the Data Incident, mitigate adverse effects and prevent a recurrence.

10.3 The details of the Data Incident response and notification procedure set forth in the Security Attachment for DocuSign Services shall apply accordingly.

11. DOCUSIGN PRIVACY CONTACT

11.1 DocuSign has appointed a Chief Privacy Officer and, in some countries, a local Data Protection Officer. Further details on how to contact the Chief Privacy Officer and, where applicable, the local Data Protection Officer are available in the DocuSign Privacy Policy on DocuSign's website at <https://www.docusign.com/company/privacy-policy>.

12. RETURN OR DISPOSAL

12.1 Prior to termination or expiration of the Agreement for any reason, Customer may delete its Personal Data Processed by the DocuSign Services in accordance with the terms of the Agreement. At Customer's prior written request and upon termination of the DocuSign Services, DocuSign will promptly return (including by providing available data retrieval functionality) or delete copies of Personal Data on DocuSign systems and DocuSign Services environments, except as otherwise stated in the Agreement or unless applicable laws require storage of the Personal Data for longer.

12.2 For Personal Data stored in Customer's service environment, or for the DocuSign Services for which no bulk data retrieval functionality is provided by DocuSign as part of the DocuSign Services, Customer is advised to take appropriate action to back up or otherwise store separately any Personal Data while the DocuSign Services environment is still active prior to termination.

EUROPEAN DPA APPENDIX

This European DPA Appendix ("EU Appendix") is incorporated into and made part of the DPA. Unless otherwise defined in this EU Appendix, capitalized terms will have the meaning given to them in the main body of the DPA.

1. DESCRIPTION OF PROCESSING

1.1 Duration. The duration of the Processing of Personal Data will be the same as the Term of the Agreement, except as otherwise agreed to in writing by the Parties or required by Applicable Data Protection Laws.

1.2 Processing Activities. DocuSign may Process Personal Data as necessary to perform the DocuSign Services, including where applicable for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing. Additionally, DocuSign may collect, retain, use, disclose and otherwise Process Personal Data for the following additional business purposes: (a) to comply with Customer's written instructions, as Customer may provide to DocuSign from time to time pursuant to the Agreement and the DPA; (b) to disclose Personal Data to its employees, contractor personnel, advisers or DocuSign Service Subprocessors who have a need to know the Personal Data in order to provide the DocuSign Services and are under confidentiality obligations at least as restrictive as those described under the Agreement; (c) to comply with Applicable Data Protection Laws or any request from a Regulatory or other governmental or regulatory body (including subpoenas or court orders) so long as DocuSign provides to Customer a copy of the request and DocuSign's description of its intended disclosure within a reasonable period of time as allowed by applicable law prior to release; and (d) to exercise or defend legal claims.

1.3 Categories of Personal Data. In order to perform the DocuSign Services, depending on the DocuSign Services Customer has ordered, DocuSign may Process some or all of the following categories of Personal Data: contact information such as name, address, telephone or mobile number, email address, and passwords; goods and services provided; unique IDs collected from mobile devices; and IP addresses.

1.4 Categories of Data Subjects. Categories of Data Subjects whose Personal Data may be Processed in order to perform the DocuSign Services may include, among others, Customer's Account Administrator, Authorized Users, representatives and end users, including without limitation Customer's employees, contractors, partners, suppliers, customers and clients.