A version of this language will be included in the contract provided to those vendors awarded. ***Highlight and respond in the appropriate locations for part of your response.***

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

AND

SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. Purpose

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: InfoSec and DPA provided to address Protected Data

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor X will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOC PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITYES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR: DocuSigned by: Beatriz Benjamin 6B85A52A083E408...

Signature

Beatri Benjamin

Printed Name

DS PA

Revenue Operations Manager

Title

January 5, 2021

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND DocuSign

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with DocuSign which governs the availability to Participating Educational Agencies of the following Product(s):

DocuSign eSignature

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: by virtue of the various agreements Vendor typically puts into place with any and all of its subcontractors

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2021 and expires on June 30th 2024.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

SECURITY ATTACHMENT for DOCUSIGN SIGNATURE

Service Attachment version date: May 25, 2018

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

1. DEFINITIONS

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

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

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

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

2. INFORMATION SECURITY PROGRAM

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

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

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

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

3. SECURITY MANAGEMENT

3.1 Maintenance of Information Security Program. DocuSign will take and implement appropriate technical and organizational measures to protect Customer Data located in DocuSign Signature and will maintain the Information Security Program in accordance with 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 Signature.

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

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

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

4. PHYSICAL SECURITY MEASURES

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

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

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

5. LOGICAL SECURITY

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

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

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

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

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

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

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

6. STORAGE, ENCRYPTION, AND DISPOSAL

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

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

6.3 Disposal. DocuSign will maintain a data disposal and re-use policy for managing assets and implement industry recognized processes and procedures for equipment management and secure media disposal.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY

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

7.2 DocuSign Signature Continuity. DocuSign's production architecture for DocuSign Signature is designed to perform secure replication in near real-time to multiple active systems in geographically distributed and physically secure data centers. DocuSign will ensure that: (a) infrastructure systems for DocuSign Signature have been designed to eliminate single points of failure and to minimize the impact of anticipated environmental risks; (b) each data center supporting DocuSign Signature includes full redundancy and fault tolerance infrastructure for

electrical, cooling, and network systems; and (c) Production Environment servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability.

8. INCIDENT RESPONSE AND BREACH NOTIFICATION

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

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

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

9. INDEPENDENT ASSURANCES AND AUDITS

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

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

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

9.4 Conditions of Audit.

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

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

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

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

DocuSign

DocuSign Data Protection Attachment

Last revised: December 4, 2020

This DocuSign Data Protection Attachment ("**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.

Except as expressly stated otherwise in the DPA, the Agreement, or the DocuSign Processor Code (defined below), in the event of any conflict between these documents, the following order of precedence applies (in descending order): (i) the Processor Code, (ii) the Standard Contractual Clauses (if applicable), (iii) the body of the DPA, (iv) any documents attached to the DPA, and (v) the Agreement.

1. Definitions

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

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

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

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

"**Process/Processing**" has the meaning set forth under Applicable Data Protection Laws as such is performed on Personal Data, 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.

"**Processor Code**" means DocuSign's Processor Privacy Code, the most current version of which is available on DocuSign's website at https://trust.docusign.com/en-us/trust-certifications/gdpr/bcr-p-processor-privacy-code/.

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

"**Third Party Subprocessor**" means a third party, other than a DocuSign Affiliate, which may Process Personal Data on behalf of DocuSign as part of the provision of DocuSign Services, as set forth in Section

"**Security Incident**" means either such term or Data Breach as defined in the Security Attachment of the Agreement for the DocuSign Service.

2. General

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

DocuSign

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 DocuSign Services provided under the Agreement. Each Party is responsible for compliance with its own respective obligations under Applicable Data Protection Laws.

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 (i) comply with its Processor obligations under Applicable Data Protection Laws; or (ii) assist Customer to comply with Customer's Controller 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 DocuSign Services payable under the Agreement. If additional charges or fees are expected, such as additional license or third party contractor fees, 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.

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 the DPA (including any attachment to the DPA) or Agreement.

3.4 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 the DPA. Additionally, each Party agrees it will take commercial 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 (i) access its DocuSign Services environment containing Personal Data to address the request, or (ii) to the extent such access is not available to Customer, contact DocuSign Customer Support for additional assistance to enable Customer to address the request.

4.2 If DocuSign directly receives any requests or inquiries from a Data Subject that has identified Customer as the Controller or that DocuSign determines that Customer is a Controller of such Personal Data, DocuSign will promptly pass on such request to Customer. 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 Controller, Customer is solely responsible for responding to such Data Subject's requests and that DocuSign has no responsibility to respond to a Data Subject for or on the Customer's behalf. Regarding any de-identified 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, link information, or take any other action which may result in such data being deemed Personal Data.

DocuSign®

5. DocuSign Affiliates and Third Party Subprocessors.

5.1 Subject to the terms of the Agreement and this DPA, Customer acknowledges and agrees that DocuSign may engage DocuSign Affiliates and/or Third Party Subprocessors to Process Personal Data of the Customer 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 Affiliate or Third Party Subprocessor.

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

5.3 Customer may object to DocuSign's use of a new Third Party Subprocessor to Process Customer's Personal Data by giving written notice to DocuSign within thirty (30) days of being informed by DocuSign of such new Third Party Subprocessor. If a Customer objects to the use of a new Third Party 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): (i) DocuSign providing a commercially reasonable alternative to avoid the Processing of Personal Data by the objected Third Party Subprocessor; or (ii) DocuSign terminating the affected DocuSign Services involving use of the new Third Party 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.

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, the Processor Code applies to the Processing of Personal Data by DocuSign as part of the provision of DocuSign Services under the Agreement. The Processor Code is incorporated by reference into this DPA, and DocuSign agrees to use commercially reasonable efforts to maintain the regulatory authorization of such Processor Code or other appropriate cross-border transfer safeguards for the duration of the Agreement. Additionally, if Customer has subscribed to be informed of changes to the Processor Code through the subscribe mechanism described in the Processor Code website, DocuSign will inform Customer of any subsequent material changes to its Processor Code through the applicable subscription alerts.

6.2 If and to the extent the Processing of Personal Data by DocuSign involves a transfer of Personal Data to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive) or (ii) not covered by the Processor Code, the Parties agree that the Standard Contractual Clauses (Controller to Processor) ("Standard Contractual Clauses"), apply to such transfers from the European Economic Area ("EEA"), Switzerland, or any country in which the applicable data protection authority has approved the use of Standard Contractual Clauses (each, an "EEA or Similar Country") to areas or recipients outside the EEA or Similar Country. If attached to this DPA, the Standard Contractual Clauses are incorporated by reference and signature of this DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including their Appendices.

DocuSign

7. Information and Assistance.

7.1 Upon prior written request, DocuSign will provide reasonable assistance and information regarding DocuSign Services provided under this Agreement to assist in (i) Customer conducting a privacy impact assessment of the DocuSign Services, and (ii) an investigation by any governmental authorities 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 accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Additional details regarding the specific security measures that apply to the DocuSign Services are as described in the Processor Code, the Standard Contractual Clauses (if applicable), and the Agreement. All DocuSign employees, as well as any Third Party Subprocessors that Process Personal Data, are subject to appropriate written confidentiality arrangements, including training on information protection, and compliance with DocuSign policies concerning protection of Confidential Information. Customer acknowledges that it is 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 that it will do so in accordance with this DPA and the Agreement in such manner that Customer deems adequate, including but not limited to maintaining appropriate security, protection, deletion, and backup of its own Personal Data.

9. Audit Rights.

9.1 The Processor Code and Agreement set forth Customer's audit rights as permitted under the DPA and to the extent required by Applicable Data Protection Laws. Additionally, Customer may request that DocuSign audit a Third Party Subprocessor (the manner of which to be determined by DocuSign in its sole discretion) and provide confirmation that such an audit occurred.

9.2 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 Reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

9.3 Unless otherwise set forth in the Agreement, each Party will bear its own costs in relation to the audit, unless DocuSign promptly informs Customer upon reviewing Customer's audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under the Agreement, such as additional license or third party contractor fees. The Parties will negotiate in good faith with respect to any such charges or fees.

9.4 Without prejudice to the rights set forth in Section 9.2 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 materially the same 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 Security Incidents. Unless notification is delayed by the actions or demands of a law enforcement agency, DocuSign shall, without undue delay, report to Customer any Security Incident following determination by

DocuSign that a Security Incident has occurred. DocuSign's obligation to report a Security 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 Security 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 Security Incident as may be required for Customer's own business and activities. 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 Security Incident.

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

11. DocuSign Privacy Contact

11.1 DocuSign has appointed a Chief Privacy Officer and, in some European 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 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 Personal Data Processed by 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 Data Protection Laws require or permit storage of the Personal Data for longer.

12.2 For Personal Data held on Customer's systems or environments, or for DocuSign Services for which no 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.

DocuSign

European DPA Addendum
to the
DocuSign Data Protection Attachment

This European DPA Addendum ("**EU Addendum**") is incorporated into and made part of the DocuSign Data Protection Attachment between Customer and DocuSign. Unless otherwise defined in this EU Addendum, 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 duration 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: (i) to comply with Customer's written instructions, as Customer may provide to DocuSign from time to time pursuant to the Agreement and this DPA; (ii) to disclose Personal Data to employees, contractor personnel, or advisers who have a need to know the Personal Data and are under confidentiality obligations at least as restrictive as those described under this DPA, or Third Party Subprocessors in order to provide the DocuSign Services; and (iii) to comply with Applicable Data Protection Laws, any request of a governmental or regulatory body (including subpoenas or court orders) or to exercise or defend legal claims.

1.3 **Categories of Personal Data**. In order to perform the DocuSign Services and 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 representatives and end users, such as Customer's employees, contractors, partners, suppliers, customers and clients.

1.5 **Additional Processing**. Additional or more specific descriptions of Processing activities, categories of Personal Data and Data Subjects may be described in the Agreement.

2. Customer Instructions

2.1 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.