Zoom Video Communications, Inc.
Global Data Processing Addendum

This Data Processing Agreement, including its Exhibits, ("**Addendum**") forms part of the Master Subscription Agreement, Terms of Service, Terms of Use or any other agreement about the delivery of the contracted services (the "**Agreement**") between Zoom Video Communications, Inc. ("**Zoom**") and the Customer named in such Agreement or identified below to reflect the parties' agreement about the Processing of Customer Personal Data (as those terms are defined below).

In the event of a conflict between the terms and conditions of this Addendum, or the Agreement, an Order Form, or any other documentation, the terms and conditions of this Addendum shall prevail with respect to the subject matter of Processing of Customer Personal Data.

All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "**Affiliate**" means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party. For purposes of this Addendum, "control" means an economic or voting interest of at least fifty percent (50%) or, in the absence of such economic or voting interest, the power to direct or cause the direction of the management and set the policies of such an entity.

1.2 "**Anonymised Data**" means, having regard to the guidance published by the European Data Protection Board, Personal Data which does not relate to an identified or identifiable natural person or rendered anonymous in such a manner that the data subject is not or no longer identifiable.

1.3 "**Applicable Data Protection Law**" means any applicable legislative or regulatory regime enacted by a recognized government, or governmental or administrative entity with the purpose of protecting the privacy rights of natural persons or households consisting of natural persons, in particular the General Data Protection Regulation 2016/679 ("GDPR") and supplementing data protection law of the European Union Member States, the United Kingdom's Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("UK GDPR"), the Swiss Federal Data Protection Act ("Swiss DPA"), Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") S.C. 2000, ch. 5, and any provincial legislation deemed substantially similar to PIPEDA under the procedures set forth therein, and the California Consumer Privacy Act ("CCPA") of 2018, the Brazilian Law No. 13,709/2018 - Brazilian General Data Protection Law ("LGPD"), the ePrivacy Directive 2002/58/EC (the "Directive"), together with any European Union Member national implementing the Directive.

1.4 "**Authorized Subprocessor**" means a subprocessor engaged by Zoom to Process Customer Personal Data on behalf of the Customer per the Customer's Instructions under the terms of the Agreement and this Addendum. Authorized Subprocessors may include Zoom Affiliates but shall exclude Zoom employees, contractors and consultants

1.5 "**Controller**" means the entity that determines as a legal person alone or jointly with others the purposes and means of the Processing of Personal Data.

1.6 "**Customer Personal Data**" means the Personal Data, including but not limited to:

(a) Content Data: All text, sound, video, or image files that are part of profile and End User information and/or exchanged between End Users (including guest users participating in Customer-hosted meetings and webinars) and with Zoom via the Services;

(b) Account Data (name, screen name and email address);

(c) Support Data (as defined in Annex I of the Standard Contractual Clauses;

(d) Website access Data (including cookies); and

(e) Diagnostic Data including but not limited to: Data from applications (including browsers) installed on End User devices **("Telemetry Data"),** Service generated server logs (with for example meeting metadata and End User settings) and Zoom internal security logs,

that are generated by, or provided to, Zoom by, or on behalf of, Customer through use of the Services as further defined in Annex I of the Standard Contractual Clauses.

1.7 **"Data Subject"** means the identified or identifiable person to whom Personal Data relates.

1.8 **"Legitimate Business Purposes"** means the exhaustive list of specific purposes for which Zoom is allowed to process some personal data as Controller as specified in Section 2.4.

1.9 **"Personal Data"** means any information relating to a Data Subject; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This includes any special categories of Personal Data defined in Art. 9 of the (UK) GDPR, data relating to criminal convictions and offences or related security measures defined in Art. 10 of the (UK) GDPR and national security numbers defined in Art. 87 of the GDPR and national supplementing law.

1.10 **"Processor"** means the entity that processes personal data on behalf of the Controller.

1.11 **"Personal Data Breach"** means a breach of security which results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data Processed by Zoom or Zoom's Authorized Subprocessor.

1.12 **"Process"** or **"Processing"** means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automatic means, such as

collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. For the avoidance of doubt: this includes processing of personal data to disclose, aggregate, pseudonymise, de-identify or anonymize Personal Data, and to combine personal data with other personal data, or to derive any data or information from such Personal Data.

1.13 **"Services"** means the Zoom Services as set forth in the Agreement or associated Zoom order form.

1.14 **"Standard Contractual Clauses"** means: (I) where the GDPR applies the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the **"EU SCCs");** (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"); and (ill) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") (the **"Swiss SCCs").**

1.15 **"Supervisory Authority"** means an independent public authority responsible for monitoring the application of Applicable Data Protection Law, including the Processing of Personal Data covered by this Addendum.

2. Processing of Personal Data: Roles, Scope and Responsibility

2.1 The Parties acknowledge and agree to the following: Customer is the Controller of Customer Personal Data. Zoom is the Processor of Customer Personal Data, except where Zoom or a Zoom affiliate acts as a Controller processing Customer Personal Data in accordance with the exhaustive list of Legitimate Business Purposes in Section 2.4.

2.2 Only to the extent necessary and proportionate, Customer as Controller instructs Zoom to perform the following activities as Processor on behalf of Customer:

(a) Provide and update the Services as licensed, configured, and used by Customer and its users, including through Customer's use of Zoom settings, administrator controls or other Service functionality;

(b) Secure and real-time monitor the Services;

(c) Resolve issues, bugs, and errors;

(d) Provide Customer requested support, including applying knowledge gained from individual customer support requests to benefit all Zoom customers but only to the extent such knowledge is anonymized; and

(e) Process Customer Personal Data as set out in the Agreement and Annex I to the Standard Contractual Clauses (subject matter, nature, purpose, and duration of Personal Data Processing in the controller to processor capacity and any other documented instruction provided by Customer and acknowledged by Zoom as constituting instructions for purposes of this Addendum.

(collectively, the **"Instructions").**

2.3 Zoom shall immediately notify the Customer, if, in Zoom's opinion, an Instruction of the Customer infringes Applicable Data Protection Law and request that Customer withdraw, amend, or confirm the relevant Instruction. Pending the decision on the withdrawal, amendment, or confirmation of the relevant Instruction, Zoom shall be entitled to suspend the implementation of the relevant Instruction.

2.4 Zoom may Process some Customer Personal Data for its own Legitimate Business Purposes, as an independent Controller, solely when the Processing is strictly necessary and proportionate, and if the Processing is for one of the following exhaustive list of purposes:

(a) Directly identifiable data (name, screen name, profile picture and email address and all Customer Personal Data directly connected to such directly identifiable data) may be Processed for:

(i) billing, account, and Customer relationship management (marketing communication with procurement/sales officials), and related Customer correspondence (mailings about for example necessary updates);

(ii) complying with and resolving legal obligations, including responding to Data Subject Requests for Personal Data processed by Zoom as data Controller (for example website data), tax requirements, agreements and disputes;

(iii) abuse detection, prevention and protection (such as automatic scanning for matches with identifiers of known Child Sexual Abuse Material ("CSAM"), virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and actions not permitted under Zoom's Community Standards (also known as an acceptable use policy);

(b) Pseudonymized and/or aggregated data (Zoom will pseudonymise and/or aggregate as much as possible and pseudonymized and/or aggregated data will not be processed on a per-Customer level); for:

(i) improving and optimizing the performance and core functionalities of accessibility, privacy, security, and the IT infrastructure efficiency of the Services, including zoom.us, explore.zoom.us, and support.zoom.us;

(ii) internal reporting, financial reporting, revenue planning, capacity planning, and forecast modeling (including product strategy);

(iii) receiving and using Feedback for Zoom's overall service improvement; and

When acting as an independent Controller, Zoom will not process Customer Personal Data for any purposes other than the above list of Legitimate Business Purposes.

2.5 Except for Zoom's free Service, Zoom will not Process Customer Personal Data for advertising purposes or serve advertising in the Services and Zoom will not process Customer Personal Data for direct marketing, profiling, research or analytics purposes except where such processing is necessary (i) to comply with Customer's instructions as set out in Section 2.2 of this DPA or (ii), only for the purposes of reporting, planning, modeling and analytics, in accordance with the Legitimate Business Purposes described in Section 2.4.

2.6 Zoom shall not ask for consent from End Users for new types of data processing, nor shall Zoom process Customer Personal Data for any "further" or "compatible" purposes (within the meaning of Articles 5(l)(b) and 6(4) GDPR) other than those specified in this Addendum or enabled by the Zoom account administrator.

2.7 With regard to content scanning for Child Sexual Abuse Material **("CSAM")** and reporting 'hits' to The National Center for Missing & Exploited Children **("NCMEC"),** Zoom shall comply with applicable regulatory guidance from the European Data Protection Board **("EDPB").** Zoom will conduct human review of matched content before it is reported. Except as otherwise provided in the Master Subscription Agreement, Zoom will immediately suspend the account of the End User and will notify the End User thereafter of the suspension and the possibility to appeal this decision.

2.8 Zoom will publish centrally accessible, exhaustive, and comprehensible documentation about the types of Customer Personal Data it collects, in particular about the Diagnostic Data. For dynamic types of data processing, Zoom will regularly update the list.

2.9 Regardless of its role as Processor or Controller, Zoom shall process all Customer Personal Data in compliance with Applicable Data Protection Laws, the "Security Measures" referenced in Section 6 of this Addendum and Annex 1 to the Standard Contractual Clauses .Zoom will follow European Data Protection Board guidance on completing a data transfer impact assessment **("DTIA")** and maintain an up-to-date DTIA applicable to the Services.

2.10 Customer shall ensure that its Instructions to Zoom comply with all laws, rules, and regulations applicable to the Customer Personal Data, and that the Processing of Customer Personal Data per Customer's Instructions will not cause Zoom to be in breach of Applicable Data Protection Law. Customer is solely responsible for the accuracy, quality, and legality of (I) the Customer Personal Data provided to Zoom by or on behalf of

Customer; (¡I) how Customer acquired any such Customer Personal Data; and (¡¡I) the Instructions it provides to Zoom regarding the Processing of such Customer Personal Data. Customer shall not provide or make available to Zoom any Customer Personal Data in violation of the Agreement, this Addendum, or otherwise in violation of Zoom's Community Standards (currently published at https://explore.zoom.us/en/community-standards/, as updated from time to time) and shall indemnify Zoom from all claims and losses in connection therewith.

2.11 Following the completion of the Services, at Customer's choice, to the extent that Zoom is a Processor, Zoom shall either enable Customer to delete some of Customer's Personal Data (for example an End User's personal data) or all of Customer's Personal Data, shall return to Customer the specified Customer Personal Data, or shall delete the specified Customer Personal Data, and delete any existing copies in compliance with its data retention and deletion policy. If return or destruction is impracticable or incidentally prohibited by a valid legal order law, Zoom shall take measures to inform the Customer and block such Customer Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by applicable law) and shall continue to appropriately protect the Customer Personal Data remaining in its possession, custody, or control and, where any Authorized Subprocessor continues to possess Customer Personal Data, require the Authorized Subprocessor to take the same measures that would be required of Zoom.

3. Privacy by design and by default

3.1 Zoom will comply with the privacy by design and data minimisation principles from the GDPR.

3.2 Zoom agrees to minimize Processing to the extent strictly necessary to provide the Services. This includes minimization of Telemetry Data, Support Data and feedback functionality, minimization of data retention periods, collection of pseudonymised identifiers when necessary, but immediate effective (irreversible) anonymization when the Service can be performed without Personal Data, offer end to end encryption when technically feasible, and the implementation and control of strict access controls to the Customer Personal Data.

3.3 Zoom shall implement policies whereby when Zoom collects new types of Diagnostic Data, such new collection shall be supervised by a privacy officer. Zoom will perform regular checks on the contents of collected Telemetry Data to verify that neither directly identifying data are collected nor Customer Content Data.

3.4 With regard to Zoom's use of cookies or similar tracking technology, Zoom shall ensure that only those cookies which are strictly necessary shall be set by default for European Enterprise and Education Customers on zoom.us, support.zoom.us and explore.zoom.us, including visits to these pages when the End User or system administrator has signed into the Zoom account.

3.5 When Zoom plans to introduce new features, or related software and services ("New Service") which will result in new types of data processing (i.e. new personal data and/or new purposes), Zoom will:

(a) Perform a data protection impact assessment.

(b) Determine if the new types of data processing following a New Service are allowed within the scope of this Addendum.

(c) Ensure that the new data processing only occurs with the necessary Customer permissions.

4. Authorized Persons

4.1 Zoom shall ensure that all persons authorized to Process Customer Personal Data and Customer Content are made aware of the confidential nature of Customer Personal Data and Customer Content and have committed themselves to confidentiality (e.g., by confidentiality agreements) or are under an appropriate statutory obligation of confidentiality.

5. Authorized Subprocessors

To the extent that Zoom is a Processor:

5.1 The Customer hereby generally authorizes Zoom to engage subprocessors in accordance with this Section 5.

5.2 Customer approves the Authorized Subprocessors listed at https://explore.zoom.us/docs/en- us/subprocessors.html:

5.3 Zoom may remove, replace, or appoint suitable and reliable further subprocessors in accordance with this Section 5.3:

(a) Zoom shall at least thirty (30) business days before the new subprocessor starts processing any Customer Personal Data notify Customer of the intended engagement (including the name and location of the relevant subprocessor, and the activities it will perform and a description of the Personal Data it will process). To enable such notifications, Customer shall visit https://explore.zoom.us/docs/en- us/subprocessors.html and enter the email address to which Zoom shall send such notifications into the submission field at the bottom of the page.

(b) In an emergency concerning Service availability or security, Zoom is not required to provide prior notification to Customer but shall provide notification within seven (7) business days following the change in subprocessor.

In either case, the Customer may object to such an engagement in writing within fifteen (15) business days of receipt of the aforementioned notice by Zoom.

5.4 If the Customer objects to the engagement of a new subprocessor, Zoom shall have the right to cure the objection through one of the following options (to be selected at Zoom's sole discretion):

(a) Zoom cancels its plans to use the subprocessor with regard to Customer Personal Data.

(b) Zoom will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the subprocessor with regard to Customer Personal Data.

(c) Zoom may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Service that would involve the use of such a subprocessor with regard to Customer Personal Data. Zoom provides Customer with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If Zoom, in its sole discretion, cannot provide any such alternative(s), or if Customer does not agree to any such alternative(s) if provided, Zoom and Customer may terminate the Agreement including the Addendum with prior written notice. Termination shall not relieve Customer of any fees or charges owed to Zoom for Services provided up to the effective date of the termination under the Agreement.

If Customer does not object to a new subprocessor's engagement within 15 business days of notice issuance from Zoom, that new subprocessor shall be deemed accepted.

5.5 Zoom shall ensure that Authorized Subprocessors have executed confidentiality agreements that prevent them from unauthorized Processing of Customer Personal Data and Customer Content both during and after their engagement by Zoom.

5.6 Zoom shall, by way of contract or other legal act, impose on the Authorized Subprocessor the equivalent data protection obligations as set out in this Addendum and detailed in the GDPR. The Parties acknowledge and agree that notice periods shall be deemed equivalent regardless of disparate notification periods. If personal data are transferred to an Authorized Subprocessor in a third country, Zoom will ensure the transferred data are processed with the same GDPR transfer guarantees as agreed with Customer (such as Standard Contractual Clauses and BCRs). Zoom will also perform a case by case assessment if supplementary measures are required in cases of onward transfers to third countries in order to bring the level of protection of the transferred data up to the ELI standard of essential equivalence.

5.7 Zoom shall be fully liable to Customer where that Authorized Subprocessor fails to fulfil its data protection obligations for the performance of that Authorized Subprocessor's

obligations to the same extent that Zoom would itself be liable under this Addendum had it conducted such acts or omissions.

6. Security of Personal Data

6.1 Zoom may not update the Services in a way that would remove Customer's choice to apply end to end encryption to Meetings, introduce any functionality that would purposefully allow anyone not authorized by the Customer to gain access to Customer encryption keys or Customer content, or remove the ability to store recordings locally.

6.2 Zoom certifies that it has not purposefully created any "back doors" or similar programming in the Services that could be used by third parties to access the system and/or personal data. Zoom has not purposefully created or changed its business processes in a manner that facilitates such third party access to personal data or systems. Zoom certifies there is no applicable law or government policy that requires Zoom as importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession of or to hand over the encryption key.

6.3 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Zoom shall maintain appropriate technical and organizational measures with regard to Customer Personal Data and to ensure a level of security appropriate to the risk, including, but not limited to, the **"Security Measures"** set out in Annex II to the Standard Contractual Clauses (attached here as EXHIBIT B). Customer acknowledges that the Security Measures are subject to technical progress and development and that Zoom may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

7. International Transfers of Personal Data

7.1 Zoom may not update the Services in a way that would remove Customer's ability to choose to store certain Personal Data at rest within the European Economic Area **("EEA").**

7.2 Customer acknowledges and agrees that Zoom may transfer and process Customer Personal Data to and in the United States. Zoom may transfer Customer Personal Data to third countries (including those outside of the EEA without an adequacy statement from the European Commission) to Affiliates, its professional advisors or its Authorized Subprocessors when a Zoom End User knowingly connects to data processing operations supporting the Services from such locations (such as when the End user travels outside of the territory of the EU). Zoom shall ensure that such transfers are made in compliance with Applicable Data Protection Law and this Addendum.

7.3 Any transfer of Customer's Personal Data made subject to this Addendum from member states of the European Union, the European Economic Area (Iceland, Liechtenstein, Norway), Switzerland or the United Kingdom to any countries where the European

Commission, the FDIPC or the UK Information Commissioner's Office has not decided that this third country or more specified sectors within that third country in question ensures an adequate level of protection, shall be undertaken, in particular, through the Standard Contractual Clauses, in connection with which the Parties agree the following:

(a) **EU SCCs (Controller to Controller Transfers).** In relation to Personal Data that is protected by the EU GDPR and processed in accordance with Section 2.4 of this Addendum, the EU SCCs shall apply, completed as follows:

(i) Module One will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 11, the optional language will not apply;

(iv) in Clause 17, Option 1 will apply, and the New EU SCCs will be governed by Irish law;

(v) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vi) Annex I of the New EU SCCs shall be deemed completed with the information set out in EXHIBIT A to this Addendum; and

(vii) Subject to Section 6.3 of this Addendum, Annex II of the EU SCCs shall be deemed completed with the information set out in EXHIBIT B to this Addendum.

(b) **EU SCCs (Controller to Processor/Processor to Processor Transfers).** In relation to Personal Data that is protected by the EU GDPR and processed in accordance with Sections 2.2 of this Addendum, the EU SCCs shall apply, completed as follows:

(i) Module Two or Module Three will apply (as applicable);

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 5.3 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the New ELI SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the ELI SCCs shall be deemed completed with the information set out in EXHIBIT A to this Addendum; and

(viii) Subject to Section 6.3 of this Addendum, Annex II of the ELI SCCs shall be deemed completed with the information set out in EXHIBIT B to this Addendum.

(c) **Transfers from the UK.** In relation to Personal Data that is protected by the UK GDPR, the UK Addendum will apply, completed as follows:

(i) The EU SCCs shall also apply to transfers of such Personal Data, subject to sub-Section (ii) below;

(ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above in Section 7.3(a)-(b) of this Addendum, and the option "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this Addendum.

(d) **Transfers from Switzerland.** In relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply in accordance with Sections 7.3(a) -(b), with the following modifications:

(i) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and

(iii) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the FDIPC and competent courts in Switzerland, unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA, in which event the Swiss SCCS shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in EXHIBITS A and B.

7.4 It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this Addendum) the Standard Contractual Clauses shall prevail to the extent of such conflict.

7.5 Zoom may adopt a replacement data export mechanism (including any new version of or successor to the Standard Contractual Clauses or alternative mechanisms adopted pursuant to Applicable Data Protection Law) **("Alternative Transfer Mechanism").** So long as the Alternative Transfer Mechanism complies with Applicable Data Protection Law and extends to the territories to which Customer Personal Data is transferred on behalf of the Customer, Customer agrees to execute documents and take other reasonably necessary actions to give legal effect to such Alternative Transfer Mechanism.

8. Rights of Data Subjects

To the extent that Zoom is a Processor:

8.1 Zoom shall promptly notify Customer upon receipt of a request by a Data Subject to exercise Data Subject rights under Applicable Data Protection Law. Zoom will advise the Data Subject to submit his or her request to Customer, and Customer will be responsible for responding to such request.

8.2 Zoom shall, taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights (regarding information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making) under Applicable Data Protection Law.

9. Disclosure of Personal Data

9.1 Zoom will not disclose or provide access to any Customer Personal Data except:

(a) as Customer directs;

(b) as described in this Addendum; or

(c) as required by law.

9.2 If a court, law enforcement authority or intelligence agency contacts Zoom with a demand for Customer Personal Data, Zoom will first assess if it is a legitimate order consistent with Zoom's Government Requests Guide. If so, Zoom will attempt to redirect this third party to request those data directly from Customer. If compelled to disclose or provide access to any Customer Personal Data to law enforcement, Zoom will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so, for example, through a so-called *gagging order*. If Zoom is prohibited by law from fulfilling its obligations under Section 9.2, Zoom shall represent the reasonable interests of Customer. This is in all cases understood to mean:

(a) Zoom shall document a legal assessment of the extent to which: (i) Zoom is legally obliged to comply with the request or order; and (ii) Zoom is effectively prohibited from complying with its obligations in respect of the Customer under this Addendum.

(b) Zoom shall only cooperate with the US issued request or order if legally obliged to do so and, where possible, Zoom shall judicially object to the request or order or the prohibition to inform the Customer about this or to follow the instructions of the Customer.

(c) Zoom shall not provide more Customer Personal Data than is strictly necessary for complying with the request or order.

(d) If Zoom becomes aware of a situation where it has reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by Zoom, its Affiliates and Authorized Subprocessors, including any requirements to disclose personal data or measures authorizing access by public authorities, will prevent Zoom from fulfilling its obligations under this Addendum, Zoom will inform Customer without undue delay after Zoom becomes aware of such a situation.

(e) Zoom will publish a transparency report twice a year.

10. Compliance Auditing

10.1 Zoom will conduct third-party audits to attest to the ISO 27001 and SOC 2 Type II frameworks as follows:

(a) Zoom will conduct at least one audit annually. Starting in 2022, Zoom will audit the Security, Availability and Privacy Criteria in the SOC-2 audit.

(b) Audits will be performed according to the standards and rules of the regulatory or accreditation body for the applicable control standard or framework.

(c) Audits will be performed by qualified, independent, third-party security auditors at Zoom's selection and expense.

10.2 Each audit will result in the generation of an audit report ("Zoom Audit Report"), which Zoom will make available to Customer upon request. The Zoom Audit Report will be Zoom's Confidential Information. Zoom will promptly remediate issues raised in any Zoom Audit Report to the satisfaction of the auditor.

10.3 At its request and cost, Customer is entitled to have an audit carried out by a mutually agreed upon auditor to demonstrate that Zoom complies with the provisions of this Data Processing Agreement and Clause 8.9 "*Documentation and compliance*" (EU SCCs) for the processing of Personal Data. Customer may exercise the right no more than once a year, except in respect of an additional audit following (i) a Zoom data breach or (ii) if specifically ordered by Customer's national Supervisory Authority.

10.4 The costs of the periodic audits are borne by the Processor. The costs of the audit at the request of Customer are borne by Customer.

10.5 Following receipt by Zoom of a request for an audit under Section 10.4, Zoom and Customer will discuss and agree in advance on

(a) the identity of an independent and suitably qualified third-party auditor to conduct the audit;

(b) the reasonable start date and duration (not to exceed two weeks in respect of any on premise audits) of any such audit;

(c) the scope, process and normative framework of the audit, including: (i) the data processing outcomes, information, and control requirements to be in scope of the audit evidence requirements; and (ii) the nature and process for satisfactory audit evidence; and

(d) the security and confidentiality controls applicable to any such audit. All audits must be conducted in accordance with recognized international auditing standards.

10.6 Nothing in this Addendum will require Zoom to provide Personal Data of other Zoom customers or access to any Zoom systems or facilities that are not involved in the provision of the contracted Services.

11. Cooperation

11.1 Zoom shall provide Customer with all required assistance and cooperation in enforcing the obligations of the Parties under Applicable Data Protection Law. To the extent that such assistance relates to the Processing of Customer Personal Data for the purpose of the performance of the Agreement, Zoom shall in any event provide Customer with such assistance relating to:

(a) The security of Customer Personal Data;

(b) Performing checks and audits;

(c) Performing Data Protection Impact Assessments ("DPIA");

(d) Prior consultation with the Supervisory Authority;

(e) Responding to requests from the Supervisory Authority or another government body;

(f) Responding to requests from Data Subjects;

(g) Reporting Customer Personal Data Breaches.

12. Security incidents and data breaches

12.1 In the event of a confirmed Personal Data Breach (at Zoom or at a subprocessor of Zoom), Zoom shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Zoom in its sole discretion deems necessary and reasonable to remediate

such violation. In the event of such a Personal Data Breach, Zoom shall, taking into account the nature of the Processing and the information available to Zoom, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying (I) the relevant Supervisory Authority and/or (ii) Data Subjects affected by such Personal Data Breach without undue delay.

12.2 In the event of a large scale, as determined by Zoom, confirmed Personal Data Breach (with Zoom or an Authorized Subprocessor of Zoom), Customer allows Zoom to independently alert and consult the relevant Supervisory Authorities in order to better inform Customer what steps the Supervisory Authorities expect.

12.3 The obligations described in Sections 12.1 and 12.2 shall not apply if a Personal Data Breach results from the actions or omissions of Customer, except where required by Applicable Data Protection Law. Zoom's obligation to report or respond to a Personal Data Breach under Sections 12.1 and 12.2 will not be construed as an acknowledgement by Zoom of any fault or liability with respect to the Personal Data Breach.

13. General

13.1 This Addendum may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

13.2 Customer and Zoom acknowledge that the other party may disclose the Standard Contractual Clauses, this Addendum, and any privacy-related provisions in the Agreement to any Supervisory Authority upon request.

13.3 Except for the changes made by this Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Agreement, an Order Form, or any other documentation, with regard to the subject matter of this Addendum, this Addendum shall prevail to the extent of that conflict.

13.4 In the event of a change in Applicable Data Protection Law or a determination or order by a Supervisory Authority or competent court affecting this Addendum or the lawfulness of any Processing activities under this Addendum, Zoom may propose amendments to this Addendum. Customer will determine if the amendments are reasonably necessary to ensure continued compliance with Applicable Data Protection Law and/or the Processing instructions herein. In that case Parties will agree the proposed amendments in writing.

13.5 The provisions of this Addendum are severable. If any phrase, clause or provision or Exhibit (including the Standard Contractual Clauses) is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this Addendum or the remainder of the Exhibit, shall remain in full force and effect.

13.6 This Addendum shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

SANTA ROSA CITY SCHOOLS

"Customer"

Signature:

Print Name:

Lisa Cavin

Title:

Associate Superintendent

Date: February 23, 2023

Customer Address:

211 Ridgway Ave, Santa Rosa, California 95401,
United States

Zoom Video Communications, Inc.

Signature: DocuSigned by: Deborah Fay

Print Name: Deborah Fay

Title: Deputy General Counsel, Commercial

EXHIBIT A

Annex I: Description of the Processing/Transfer

Controller to Controller

(A) List of Parties:

Data Exporter	Data Importer
Name: SANTA ROSA CITY SCHOOLS	Name: Zoom Video Communications, Inc.
Address: 211 Ridgway Ave, Santa Rosa, California 95401, United States	Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113
Contact Person's Name, position and contact details: Name: Position: Address: 211 Ridgway Ave, Santa Rosa, California 95401, United States	Contact Person's Name, position and contact details: Name: Deborah Fay Position: Data Protection Officer Address: 55 Almaden Blvd., Suite 600, San Jose, CA95113
Activities relevant to the transfer: See Section (B) below	Activities relevant to the transfer: See Section (B) below
Role: Controller	Role: Controller

(B) Description of Transfer

Categories Data Subjects	
The personal data transferred concern the following categories of data subjects:	End Users
Purposes of the transfer(s)	
The transfer is made for the following purposes:	Notwithstanding the purposes for which Zoom is permitted to process Personal Data as a Processor as set out in Annex 1 (controller to processor), Zoom is permitted to process some Customer Personal Data for its own Legitimate Business Purposes, as an independent Controller, solely when the processing is strictly necessary and proportionate, for the following exhaustive list of purposes: Directly identifiable data (name, screen name, profile picture and email address and all Customer Content Data directly connected to such directly identifiable data) for: • billing, account, and customer relationship management (marketing communication with procurement/sales officials), and related Customer correspondence (mailings about for example necessary updates);

	• complying with and resolving legal obligations, including responding to Data Subject Requests for Personal Data processed by Zoom as data controller (for example website data), tax requirements, agreements and disputes; • abuse detection, prevention and protection (such as automatic scanning for matches with identifiers of known Child Sexual Abuse Material ("CSAM"), virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and actions not permitted under Zoom's Community Standards (also known as an acceptable use policy); Pseudonymised and/or aggregated data (Zoom will pseudonymise and/or aggregate as much as possible and pseudonymized and/or aggregated data will not be processed on a per-Customer level); for: • improving and optimizing the performance and core functionality of accessibility, privacy, security and IT infrastructure efficiency of the Services, including zoom.us, explore.zoom.us and support.zoom.us; • internal reporting, financial reporting, revenue planning, capacity planning and forecast modeling (including product strategy); and • receiving and using Feedback for Zoom's overall service improvement.
Categories of Personal Data	

The personal data transferred concern the following categories of data:	**Customer Content Data:** **Zoom Account Profile Info**: Data associated with the end user's Zoom account, profile picture, password, company name, and Customer's preferences. This will include: • Zoom unique user ID, • profile picture (optional) **Diagnostic Data:** **Meeting metadata**: Metrics about Service usage, including when and how meetings were conducted). This category includes: • event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, user ID, and meeting ID) • meeting session information, including frequency, average and actual duration, quantity, quality, network activity, and network connectivity • number of meetings • number of screen-sharing and non-screen-sharing sessions • number of participants • meeting host information • host name • meeting site URL • meeting start/end Time • join method • performance, troubleshooting and diagnostics information **Telemetry data:** Data collected from locally installed software (applications and browser information about the deployment of Zoom Services and related systems environment / technical information. This includes: • PC name • microphone • speaker • camera • domain • hard disc ID • network type • operating system type and version • client version • MAC address

	• event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, • user ID and meeting ID) • service logs (information on systems events and states) **Other Service Generated Data:** • spam identification • push notifications • Zoom persistent unique identifiers such as UUID or user ids that are combined with other data elements including: • IP address • Data center • PC name • Microphone • Speaker • Camera • Domain • Hard disc ID • Network type • Operating System Type and Version • Client Version • IP Addresses along the Network Path **Support Data:** • problem description, post-meeting feedback
Frequency of the transfer	
Whether continuous or one-off.	The transfer of account information is one off, otherwise continuous when using the Service
Special categories of personal data (if appropriate)	
The personal data transferred concern the following categories of sensitive data:	Not applicable if end to end encryption is enabled, and if End Users do not upload profile pictures revealing special categories of data
Duration of processing:	In accordance with the retention period detailed below.
Nature and Subject Matter of the Processing:	Zoom will process Customer Personal Data for its own exhaustive list of Legitimate Business Purposes when strictly necessary and proportionate, in accordance with the Addendum.

Retention period (or, if not possible to determine, the criteria used to determine that period):	Zoom retains Customer Personal Data for as long as required for its own exhaustive list of Legitimate Business Purposes, in accordance with the Addendum. The criteria used to determine Zoom's retention periods include the following: • The length of time of Zoom's relationship with Service users (for example, the duration of a Zoom account) • Whether account owners modify or their users delete information through their accounts • Whether Zoom has a legal obligation to keep the data (for example, certain laws require Zoom to keep records for a certain period of time) • Whether retention is required by Zoom's legal position (such as in regard to the enforcement of agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).

(C): Competent supervisory authority

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to Personal Data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (the "ICO"). With respect to Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

Controller to Processor

(A) List of Parties:

Data Exporter	Data Importer
Name: SANTA ROSA CITY SCHOOLS	Name: Zoom Video Communications, Inc.
Address: 211 Ridgway Ave, Santa Rosa, California 95401, United States	Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113
Contact Person's Name, position and contact details: Name: Position: Address: 211 Ridgway Ave, Santa Rosa, California 95401, United States	Contact Person's Name, position and contact details: Name: Deborah Fay Position: Data Protection Officer Address: 55 Almaden Blvd., Suite 600, San Jose, CA95113
Activities relevant to the transfer: See Section (B) below	Activities relevant to the transfer: See Section (B) below
Role: Controller	Role: Processor

(B) Description of Transfer

Categories Data Subjects	
The personal data transferred concern the following categories of data subjects:	Individuals about whom Personal Data is provided to Zoom via the Services by (or at the direction of) Customer or End Users, which may include without limitation Customer's or its Affiliates' employees, contractors, and End Users.
Purposes of the transfer(s)	
The transfer is made for the following purposes:	Zoom will only process Customer Personal Data as Processor for the following purposes and only when necessary and proportionate to comply with the Customer's instructions: • Providing and updating the Services as licensed, configured, and used by Customer and its users, including through Customer's use of Zoom settings, administrator controls or other Service functionality; • Securing and real-time monitoring the Services; • Resolving issues, bugs, and errors; billing, account, and customer relationship management (marketing communication with procurement/sales officials), and related Customer correspondence (mailings about for example necessary updates); • Providing customer requested support, including applying knowledge gained from individual customer support requests to benefit all Zoom customers but only to the extent such knowledge is anonymized. • as set out in the Agreement and Annex I to the SCCs detailing the subject matter, nature, purpose, and duration of Personal Data Processing in the controller to processor capacity. • any other documented instruction provided by Customer and acknowledged by Zoom as constituting instructions for purposes of this Addendum.
Categories of Personal Data	

The personal data transferred concern the following categories of data:	**Customer Content Data:** **Zoom Account Profile Info**: Data associated with the end user's Zoom account, profile picture, password, company name, and Customer's preferences. This will include: • Zoom unique user ID, • social media login (optional), • profile picture (optional) and • display name. **Customer authentication data**: This will include username and password unless Single Sign On (SSO) is used **Meeting and webinar communication content**. This will include: • video, audio, whiteboard, captions, and presentations • in-meeting Questions & Answers, polls, and survey information • closed captioning (Live Transcription) **Chat Messages**. 1:1 in-meeting and group chat messages that are not transferred to a permanent chat channel. **Customer Initiated cloud recordings**. This will include the following recordings if such recording is permitted by the Customer administrator controls and selected by a meeting host or participant: • video recording of video, audio, whiteboard, captions, and presentations • audio recording • text file of all in meeting group chats • audio transcript text file • in-meeting Questions & Answers, polls, and survey information • closed captioning transcripts **Meeting and webinar participant information**. This includes: • registered participant name and contact details; and any data requested by Customer to be provided in conjunction with registration, email addresses • status of participant (as host, as participants in a chat or as attendees) • room names (if used) • user categorizations • tracking fields such as department or group • scheduled time for a meeting • topic names **Stored Chat Information**. This is data at rest (in storage) and will include: • chat messages • files exchanged via chat • images exchanged via chat • videos exchanged via chat • chat channel title • whiteboard annotations

	Address book Information. This includes contact information made available through Customer controlled integrations (e.g. Outlook) **Calendar Information**. This includes meeting schedules made available through Customer controlled integrations (e.g. Outlook, Google Calendar) **Diagnostic Data**: **Meeting metadata**: Metrics about Service usage, including when and how meetings were conducted). This category includes: • event logs (including: action taken, event type and subtype, in-app event location, timestamp, client UUID, user ID, and meeting ID) • meeting session information, including frequency, average and actual duration, quantity, quality, network activity, and network connectivity • number of meetings • number of screen-sharing and non screen-sharing sessions • number of participants • meeting host information • host name • meeting site URL • meeting start/end Time • join method **Telemetry data**: Data collected from locally installed software (applications and browser information about the deployment of Zoom Services and related systems environment / technical information. This includes: • PC name • microphone • speaker • camera • domain • hard disc ID • network type • operating system type and version • client version • MAC address • event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, • user ID and meeting ID) • service logs (information on systems events and states) **Other Service Generated Data**: • spam identification • push notifications • Zoom persistent unique identifiers such as UUID or user ids that are combined with other data elements including: • IP address • Data center • PC name

	• Microphone • Speaker • Camera • Domain • Hard disc ID • Network type • Operating System Type and Version • Client Version • IP Addresses along the Network Path **Support Data**: • Contact name of support requestor, time, subject, problem description, post-meeting feedback (thumbs- up/down) • User supplied attachments including recordings, transcripts or screenshots, post-meeting feedback (open text provided with thumbs down)
Frequency of the transfer	
Whether continuous of one off.	Continuous
Special categories of personal data (if appropriate)	
The personal data transferred concern the following categories of sensitive data:	Special categories of data are not required to use the service. The Customer / data exporter can prevent the processing of these data by using end to end encryption in the Meetings and preventing End Users from uploading profile information that contains such special categories of data. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning an individual's health or sex life.
Duration of processing:	The term of the Agreement plus the period until Zoom deletes all Customer Personal Data processed on behalf of Customer in accordance with the Agreement.
Nature and Subject Matter of the Processing:	Zoom will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Addendum

Retention period (or, if not possible to determine, the criteria used to determine that period):	Zoom retains Customer Personal Data for as long as required for its own exhaustive list of Legitimate Business Purposes, in accordance with the Addendum. The criteria used to determine Zoom's retention periods include the following: • The length of time of Zoom's relationship with Service users (for example, the duration of a Zoom account) • Whether account owners modify or their users delete information through their accounts • Whether Zoom has a legal obligation to keep the data (for example, certain laws require Zoom to keep records for a certain period of time) • Whether retention is required by Zoom's legal position (such as in regard to the enforcement of agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).

(C) Competent supervisory authority

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to Personal Data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (the "ICO"). With respect to Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

EXHIBIT B

Technical and Organizational Security Measures

Zoom's technical and organizational security measures for Processing Customer Personal Data will meet the Minimum-Security Control Requirements set out in this Annex II ("**Security Measures**"). Customer recognizes that there may be multiple acceptable approaches to accomplish a particular minimum control requirement. Zoom must document in reasonable detail how a particular control meets the stated minimum control requirement. Zoom may revise the Security Measures from time to time. The term "should" in these Security Measures means that Zoom will use commercially reasonable efforts to accomplish the stated minimum control requirement and will document those efforts in reasonable detail, including the rationale, if any, for deviation.

As used in these Security Measures, (i) "including" and its derivatives mean "including but not limited to"; and (ii) any capitalized terms not defined in this Annex II shall have the same meaning as set forth in the Addendum.

1. Definitions

1.1 "**Systems**" means Zoom's production systems.

1.2 "**Assets**" means Zoom's production assets.

1.3 "**Facilities**" means Zoom's production facilities, whether owned or leased by Zoom (e.g., AWS, data centers).

2. Risk Management

2.1 Risk Assessment Program. The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.

2.2 Risk Assessment. A risk assessment must be performed annually to verify the implementation of controls that protect business operations and Customer Content.

3. Security Policy

3.1 A documented set of rules and procedures must regulate the Processing of information and associated services.

3.2 Security Policies and Exception Process. Security policies must be documented, reviewed, and approved, with management oversight, on a periodic basis, following industry best practices.

3.3 A risk-based exception management process must be in place for prioritization, approval, and remediation or risk acceptance of controls that have not been adopted or implemented.

3.4 Awareness and Education Program. Security policies and responsibilities must be communicated and socialized within the organization to Zoom personnel. Zoom personnel must receive security awareness training on an annual basis.

4. Organizational Security

4.1 A personnel security policy must be in place to establish organizational requirements to ensure proper training, competent performance, and an appropriate and accountable security organization.

4.2 Organization. Current organizational charts representing key management responsibilities for services provided must be maintained.

4.3 Background Checks. Where legally permissible, background checks (including criminal) must be performed on applicable Zoom personnel.

4.4 Confidentiality Agreements. Zoom personnel must be subject to written non-disclosure or confidentiality obligations.

5. Technology Asset Management

5.1 Controls must be in place to protect Zoom production assets, including mechanisms to maintain an accurate inventory of assets and handling standards for introduction and transfer, removal and disposal of assets.

5.2 Accountability. A process for maintaining an inventory of hardware and software assets and other information resources, such as databases and file structures, must be documented. Process for periodic asset inventory reviews must be documented. Identification of unauthorized or unsupported hardware/software must be performed.

5.3 Asset Disposal or Reuse. If applicable, Zoom will use industry standards to wipe or carry out physical destruction as the minimum standard for disposing of assets. Zoom must have documented procedures for disposal or reuse of assets.

5.4 Procedures must be in place to remove data from production systems in which Customer's Personal Data are stored, processed, or transmitted.

6. Physical and Environmental

6.1 Controls must be in place to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.

6.2 Physical and Environmental Security Policy. Physical and environmental security plans must exist for facilities and scenarios involving access or storage of Customer's Personal Data. Additional physical and environmental controls must be required and enforced for applicable facilities, including servers and datacenter locations.

6.3 Physical Access. Physical access, to include visitor access to facilities, must be restricted and all access periodically reviewed.

6.4 Policies must be in place to ensure that information is accessed on a need-to-know basis.

6.5 Environmental Control. Facilities, including data and processing centers, must maintain appropriate environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection. Environmental control components must be monitored and periodically tested.

7. Communication and Connectivity

7.1 Zoom must implement controls over its communication network to safeguard data. Controls must include securing the production network and implementation of encryption, logging and monitoring, and disabling communications where no business need exists.

7.2 Network Identification. A production network diagram, to include production devices, must be kept current to facilitate analysis and incident response.

7.3 Data Flow Diagram. A current data flow diagram must depict data from origination to endpoint (including data which may be shared with subprocessors).

7.4 Data Storage. All of Customer's Personal Data, including Customer's Personal Data shared with subprocessors, must be stored and maintained in a manner that allows for its return or secure destruction upon request from Customer.

7.5 Firewalls. Firewalls must be used for the isolation of all environments, to include physical, virtual, network devices, production and non-production, and application/presentation layers. Firewall management must follow a process that includes restriction of administrative access, and that is documented, reviewed, and approved, with management oversight, on a periodic basis.

7.6 The production network must be either firewalled or physically isolated from the development and test environments. Multi-tier security architectures that segment application tiers (e.g., presentation layer, application and data) must be used.

7.7 Periodic network vulnerability scans must be performed, and any critical vulnerabilities identified must be remediated within a defined and reasonable timeframe.

7.8 Clock Synchronization. Production network devices must have internal clocks synchronized to reliable time sources.

7.9 Remote Access. The data flow in the remote connection must be encrypted and multi-factor authentication must be utilized during the login process.

7.10 Remote connection settings must limit the ability of remote users to access both initiating network and remote network simultaneously (i.e., no split tunneling).

7.11 Subprocessors' remote access, if any, must adhere to the same controls and must have a valid business justification.

7.12 Wireless Access. Wireless access to the Zoom corporate network must be configured to require authentication and be encrypted.

8. Change Management

8.1 Changes to the production systems, production network, applications, data files structures, other system components, and physical/environmental changes must be monitored and controlled through a formal change control process. Changes must be reviewed, approved, and monitored during post implementation to ensure that expected changes and their desired result are accurate.

8.2 Change Policy and Procedure. A change management policy, including application, operating system, network infrastructure, and firewall changes must be documented, reviewed, and approved, with management oversight, on a periodic basis.

8.3 The change management policy must include clearly identified roles and responsibilities so as to support separation of duties (e.g., request, approve, implement). The approval process must include pre- and postevaluation of change. Zoom posts service status and scheduled maintenance at https://status.zoom.us.

9. Operations

9.1 Documented operational procedures must ensure the correct and secure operation of Zoom's assets. Operational procedures must be documented and include monitoring of capacity, performance, service level agreements and key performance indicators.

10. Access Control

10.1 Authentication and authorization controls must be appropriately robust for the risk of the system, data, application, and platform; access rights must be granted based on the principle of least privilege and monitored to log access and security events, using tools that enable rapid analysis of user activities.

10.2 Logical Access Control Policy. Documented logical access policies and procedures must support role-based, "need-to-know" access (e.g., interdepartmental transfers, terminations) and ensure separation of duties during the approval and provisioning process. Each account provisioned must be uniquely identified. User access reviews must be conducted on a periodic basis.

10.3 Privileged Access. Management of privileged user accounts (e.g., those accounts that have the ability to override system controls), to include service accounts, must follow a documented process and be restricted. A periodic review and governance process must be maintained to ensure appropriate provisioning of privileged access.

10.4 Authentication and Authorization. A documented authentication and authorization policy must cover all applicable systems. That policy must include password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized. Authentication credentials must be encrypted, including in transit to and from subprocessors' environments or when stored by subprocessors.

11. Data Integrity

11.1 Controls must ensure that any data stored, received, controlled, or otherwise accessed is accurate and reliable. Procedures must be in place to validate data integrity.

11.2 Data Transmission Controls. Processes, procedures, and controls must be documented, reviewed, and approved, with management oversight, on a periodic basis, to ensure data integrity during transmission and to validate that the data transmitted is the same as data received.

11.3 Data Transaction Controls. Controls must be in place to protect the integrity of data transactions at rest and in transit.

11.4 Encryption. Data must be protected and should be encrypted, both in transit and at rest, including when shared with subprocessors.

11.5 Data Policies. A policy must be in place to cover data classifications, encryption use, key and certificate lifecycle management, cryptographic algorithms and associated key lengths. This policy must be documented, reviewed, and approved with management oversight, on a periodic basis.

11.6 Encryption Uses. Customer Personal Data must be protected, and should be encrypted, while in transit and at rest. Customer Content must be protected, and should be encrypted when stored and while in transit over any network; authentication credentials must be encrypted at all times, in transit or in storage.

12. Incident Response

12.1 A documented plan and associated procedures, to include the responsibilities of Zoom personnel and identification of parties to be notified in case of an information security incident, must be in place.

12.2 Incident Response Process. The information security incident management program must be documented, tested, updated as needed, reviewed, and approved, with management oversight, on a periodic basis. The incident management policy and procedures must include prioritization, roles and responsibilities,procedures for escalation (internal) and notification, tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity.

13. Business Continuity and Disaster Recovery

13.1 Zoom must have formal documented recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to the business unit, support group unit, application, or infrastructure component. Plans assure timely and orderly recovery of business, support processes, operations, and technology components within an agreed upon time frame and include orderly restoration of business activities when the primary work environment is unavailable.

13.2 Business Recovery Plans. Comprehensive business resiliency plans addressing business interruptions of key resources supporting services, including those provided by subprocessors, must be documented, tested, reviewed, and approved, with management oversight, on a periodic basis. The business resiliency plan must have an acceptable alternative work location in place to ensure service level commitments are met.

13.3 Technology Recovery. Technology recovery plans to minimize service interruptions and ensure recovery of systems, infrastructure, databases, applications, etc. Must be documented, tested, reviewed, and approved with management oversight, on a periodic basis.

14. Back-ups

14.1 Zoom must have policies and procedures for back-ups of Customer's Personal Data. Backups must be protected using industry best practices.

14.2 Back-up and Redundancy Processes. Processes enabling full restoration of production systems, applications, and data must be documented, reviewed, and approved, with management oversight, on a periodic basis.

15. Third-Party Relationships

15.1 Subprocessors must be identified, assessed, managed, and monitored. Subprocessors that provide material services, or that support Zoom's provision of material services to Customers, must comply with control requirements no less stringent than those outlined in this document.

15.2 Selection and Oversight. Zoom must have a process to identify subprocessors providing services to Zoom; these subprocessors must be disclosed to Customer and approved to the extent required by this Agreement.

15.3 Lifecycle Management. Zoom must establish contracts with subprocessors providing material services; these contracts should incorporate security control requirements, including data protection controls and notification of security and privacy breaches must be included. Review processes must be in place to ensure subprocessors' fulfillment of contract terms and conditions.

16. Standard Builds

16.1 Production systems must be deployed with appropriate security configurations and reviewed periodically for compliance with Zoom's security policies and standards.

16.2 Secure Configuration Availability. Standard security configurations must be established and security hardening demonstrated. Process documentation must be developed, maintained, and under revision control, with management oversight, on a periodic basis. Configurations must include security patches, vulnerability management, default passwords, registry settings, file directory rights and permissions.

16.3 System Patches. Security patch process and procedures, to include requirements for timely patch application, must be documented.

16.4 Operating System. Versions of operating systems in use must be supported and respective security baselines documented.

16.5 Desktop Controls. Systems must be configured to provide only essential capabilities. The ability to write to removable media must be limited to documented exceptions.

17. Application Security

17.1 Zoom must have an established software development lifecycle for the purpose of defining, acquiring, developing, enhancing, modifying, testing, or implementing information systems. Zoom must ensure that web-based and mobile applications used to store, receive, send, control, or access Customer Personal Data are monitored, controlled, and protected.

17.2 Functional Requirements. Applications must implement controls that protect against known vulnerabilities and threats, including Open Web Application Security Project (OWASP) Top 10 Risks and denial of service (DDOS) attacks.

17.3 Application layer controls must provide the ability to filter the source of malicious traffic.

17.4 Restrictions must also be placed on or in front of web server resources to limit denial of service (DoS) attacks.

17.5 Zoom must monitor uptime on a hosted web or mobile application.

17.6 Software Development Life Cycle. A Software Development Life Cycle (SDLC) methodology, including release management procedures, must be documented, reviewed, approved, and version-controlled, with management oversight, on a periodic basis. These must include activities that foster the development of secure software.

17.7 Testing and Remediation. Software executables related to client/server architecture that are involved in handling Customer Personal Data must undergo vulnerability assessments (both the client and server omponents) prior to release and on an on-going basis, either

internally or using external experts, and any gaps identified must be remediated in a timely manner.

(a) Testing must be based on, at a minimum, the OWASP Top 10 risks (or the OWASP Mobile Top 10 risks, where applicable), or comparable replacement.

(b) Zoom must conduct penetration testing on an annual basis.

18. Vulnerability Monitoring

18.1 Zoom must continuously gather information and analyze vulnerabilities in light of existing and emerging threats and actual attacks. Processes must include vulnerability scans, anti-malware, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), logging and security information and event management analysis and correlation.

18.2 Vulnerability Scanning and Issue Resolution. Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically and prior to system provisioning for production systems that process, store or transmit Customer Content.

18.3 Malware. In production, Zoom must employ tools to detect, log, and disposition malware.

18.4 Intrusion Detection/Advanced Threat Protection. Network and host-based intrusion detection/advanced threat protection must be deployed with events generated fed into centralized systems for analysis. These systems must accommodate routine updates and realtime alerting. IDS/advanced threat protection signatures must be kept up to date to respond to threats.

18.5 Logging and Event Correlation. Monitoring and logging must support the centralization of security events for analysis and correlation. Organizational responsibility for responding to events must be defined. Retention schedule for various logs must be defined and followed.

18.6 Zoom publishes a vulnerability disclosure policy at https://explore.zoom.us/docs/en-us/vulnerabilitydisclosure-policy.html.

19. Cloud Technology

19.1 Adequate safeguards must ensure the confidentiality, integrity, and availability of Customer Personal Data stored, processed or transmitted using cloud technology (either as a cloud customer or cloud provider, to include subprocessors), using industry standards.

19.2 Audit Assurance and Compliance. The cloud environment in which data is stored, processed or transmitted must be compliant with relevant industry standards and regulatory restrictions.

19.3 Application and Interface Security. Threat modeling should be conducted throughout the software development lifecycle, including vulnerability assessments, including

Static/Dynamic scanning and code review, to identify defects and complete remediations before hosting in cloud environments.

19.4 Business Continuity Management and Operational Resiliency. Business continuity plans to meet recovery time objectives (RTO) and recovery point objectives (RPO) must be in place.

19.5 Data Security and Information Lifecycle Management. Proper segmentation of data environments and segregation must be employed; segmentation/segregation must enable proper sanitization, per industry requirements.

19.6 Encryption and Key Management. All communications must be encrypted in-transit between environments.

19.7 Governance and Risk Management. Comprehensive risk assessment processes and centralized monitoring that enables incident response and forensic investigation must be used to ensure proper governance and oversight.

19.8 Identity and Access Management. Management of accounts, including accounts with privileged access, must prevent unauthorized access and mitigate the impacts thereof.

19.9 Infrastructure and Virtualization Security. Controls defending against cyberattacks, including the principle of least privilege, baseline management, intrusion detection, host/network-based firewalls, segmentation, isolation, perimeter security, access management, detailed data flow information, network, time, and a SIEM solution must be implemented.

19.10 Supply Chain Management, Transparency and Accountability. Zoom must be accountable for the confidentiality, availability and integrity of production data, to include data processed in cloud environments by subprocessors.

19.11 Threat and Vulnerability Management. Vulnerability scans (authenticated and unauthenticated) must be performed, both internally and externally, for production systems. Processes must be in place to ensure tracking and remediation.

20. Audits

20.1 At least annually, Zoom will conduct an independent third-party review of its security policies, standards, operations, and procedures related to the Services provided to Customer. Such review will be conducted in accordance with the AICPA's Statements on Standards for Attestation Engagements (SSAE), and Zoom will be issued a SOC 2 Type II report. Upon Customer's request, Zoom will provide Customer with a copy of the SOC 2 Type II report within thirty (30) days. If applicable, Zoom will provide a bridge letter to cover time frames not covered by the SOC 2 Type II audit period scope within 30 days, upon request by Customer. If exceptions are noted in the SOC 2 Type II audit, Zoom will document a plan to promptly address such exceptions and shall implement corrective

measures within a reasonable and specific period. Upon Customer's reasonable request, Zoom will keep Customer informed of progress and completion of corrective measures.

20.2 Customer shall rely on the third-party audit SOC 2 Type II report for validation of proper information security practices and shall not have the right to audit, unless such right is granted under applicable law, except in the case of a Security Breach resulting in a material business impact to Customer. If Customer exercises the right to audit as a result of a Security Breach, such audit shall be within the scope of the Services. Customer will provide Zoom a minimum of thirty (30) days of notice prior to the audit. Zoom shall have the right to approve any third-party Customer may choose to conduct or be involved in the audit.

21. Specific Measures

Measure	Description
Measures of pseudonymisation and encryption of personal data	• *Optional End-to-End Encryption for Meetings:* Users may choose to enable end-to-end encryption for Zoom meetings. This provides a high level of security since no third party — including Zoom — has access to the meeting's private keys. • *Default Encryption:* The connection between a given device and Zoom is encrypted by default, using a mixture of TES 1.2+ (Transport Layer Security), Advanced Encryption Standard (AES) 256-bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used depend on whether a user uses the Zoom client, a web browser, a third-party device or service, or the Zoom phone product. For further information, please see our Encryption Whitepaper
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Zoom utilizes security measures to ensure the ongoing confidentiality, integrity, availability, and resilience of our processing systems and services.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Zoom takes measures to facilitate the restoration of availability and access to our processing systems and services promptly in the event of a physical or technical incident.
Processes for regularly testing, assessing and evaluating the effectiveness of	Zoom implements a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the data we process.

technical and organisational measures in order to ensure the security of the processing	
Measures for user identification and authorisation	*Protections against unauthorised meeting participants*: Zoom has implemented numerous safeguards and controls to prohibit unauthorized participants from joining meetings: • Eleven (11) digit unique meeting IDs • Complex passwords • Waiting rooms with the ability to automatically admit participants from • your domain name or another selected domain • Meeting lock feature that can prevent anyone from joining the meeting • Ability to remove participants • Authentication profiles that only allow entry to registered users, or restrict to specific email domains
Measures for the protection of data during transmission	• *Optional End-to-End Encryption for Meetings*: Users may choose to enable end-to-end encryption for Zoom meetings. This provides a high level of security since no third party — including Zoom — has access to the meeting's private keys. • *Default Encryption*: The connection between a given device and Zoom is encrypted by default, using a mixture of TLS 1.2+ (Transport Layer Security), Advanced Encryption Standard (AES) 256-bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used depend on whether a user uses the Zoom client, a web browser, a third-party device or service, or the Zoom phone product. For further information, please see our Encryption Whitepaper.
Measures for the protection of data during storage	• *Cloud Recording Storage*: Cloud Recordings are processed and stored in Zoom's cloud after the meeting has ended; these recordings can be passcode-protected or available only to people in your organization. If a meeting host enables cloud recording and audio transcripts, both will be stored encrypted. • *File transfer* storage: If a meeting host enables file transfer through inmeeting chat, those shared files will be stored encrypted and will be deleted within 31 days of the meeting. • *Cloud recording access*: Recording access for a meeting is limited to the meeting host and account admin. The

	meeting/webinar host authorizes others to access the recording with options to share publicly, internal- only, add registration to view, enable/disable ability to download, and an option to protect the recording. • *Authentication*: Zoom offers a range of authentication methods such as SAML, Google Sign-in and Facebook Login, and/or Password based which can be individually enabled/disabled for an account. • 2-*Factor* Authentication *("2FA")*: Admins can enable 2FA for your users, requiring them to set up and use 2FA to access the Zoom web portal.
Measures for ensuring physical security of locations at which personal data are processed	Controls are in place to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.
Measures for ensuring events logging	Zoom implements a standard requiring all systems to log relevant security access events.
Measures for ensuring system configuration, including default configuration	Zoom implements a standard specifying the minimum requirements for configuration management as it applies to Zoom's corporate and commercial environment.
Measures for internal IT and IT security governance and management	Zoom implements policies and standards governing internal IT and IT security governance and management.
Measures for certification/assurance of processes and products	Zoom implements a Security Audit and Accountability policy.
Measures for ensuring data minimisation	Zoom implements a privacy review in its software development lifecycle to align product development with the principle of data minimization.
Measures for ensuring data quality	Zoom implements a System and Information Integrity Policy.
Measures for ensuring limited data retention	We retain personal data for as long as required to engage in the uses described in our Privacy Statement, unless a longer retention period is required by applicable law. The criteria used to determine our retention periods include the following:

	• The length of time we have an ongoing customer relationship; • Whether account owners modify or their users delete information through their accounts; • Whether we have a legal obligation to keep the data (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or • Whether retention is advisable in light of our legal position (such as in regard to the enforcement of our agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).
Measures for ensuring accountability	Zoom implements a Security Audit and Accountability policy.
Measures for allowing data portability and ensuring erasure]	Zoom's paying customers can access their account data through their dashboard.