WISCONSIN STUDENT DATA PRIVACY AGREEMENT

School District/Local Education Agency: Green Bay Area Public School District

AND

Provider: Zoom Video Communication, Inc.

Date: July 20, 2020

This Wisconsin Student Data Privacy Agreement ("DPA") has entered, or intends to enter, into a Service Agreement (as defined below) by and between the GREEN BAY AREA PUBLIC SCHOOL DISTRICT (hereinafter referred to as "LEA") and Zoom Video Communication, Inc. (hereinafter referred to as "Provider"). The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to any agreement where Provider is to provide video communication services and other related services to LEA ("Service Agreement", which includes Provider's Privacy Policy); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services may also be subject to Wisconsin state student privacy laws, including pupil records law under Wis. Stat. § 118.125 and notice requirements for the unauthorized acquisition of personal information under Wis. Stat. § 134.98; and

WHEREAS, for the purposes of this DPA, Provider is a school district official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in Wisconsin the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, and applicable Wisconsin law, all as may be amended from time to time. In performing these services, the Provider shall be considered a School District Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA in

connection with the obligations defined in this DPA and to the extent under applicable student privacy laws. For clarity, no audit rights are provided by this DPA unless otherwise expressly described herein.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

Video conferencing services

3. Student Data to Be Provided. The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".
See Zoom Privacy Policies at https://zoom.us/privacy

4. DPA Definitions. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. "Student Data" is any data or content originated by LEA, or an End User, and stored or transmitted using the Services. Student Data includes files, documents, recordings, chat logs, meeting subject and attendees, transcripts, and any other information Customer or End Users may upload into the Services in connection with the use of the Services. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The

Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School District Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 30 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider will provide LEA (or its designee) access to retrieve , transfer said pupil generated content to a District account, for 30 days after the termination of the Service Agreement, after which time Student Data will be deleted according to regularly scheduled deletion protocols; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA as soon as possible in advance of a compelled disclosure to a Third Party.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA, as well as state and federal law.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Annual Notification of Rights**. The LEA shall include a specification of criteria under FERPA for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data

or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, not in accordance with the Service Agreement or without the express written consent of the LEA.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure**. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement or comply with applicable law.

5. **Disposition of Data**. Upon Termination of the Service Agreement, Provider shall return or delete the Student Data, except as required to be retained by law, rule or regulation that is binding upon Provider or, if the Student Data is in the possession of an Subprocessors, as required to be retained by an Subprocessor by law, rule or regulation that is binding upon the Subprocessor. If return or destruction is impracticable or prohibited by law, rule or regulation, Provider shall take measures to block such Student Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Student Data remaining in its possession, custody, or control and, where any Subprocessor continues to possess Student Data, require the Subprocessor to take the same measures that would be required of Provider. Disposition shall include (1) the shredding of any hard copies of any student data; (2) erasing; or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide, upon request, written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will promptly provide the LEA with any specified portion of the Student Data within 30 calendar days of receipt of said request. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of Student Data shall be subject to the conditions as described in Article IV, section 5 above. Further, partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above and any applicable law binding on Provider.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider will provide LEA (or its

designee) access, for 30 days after the termination of the Service Agreement or, to retrieve or transfer data to a separate account, pursuant to Article II, section 3, above, after which time Student Data will be deleted according to regularly scheduled deletion protocols. In no event shall Provider dispose of data pursuant to this provision unless and until Provider provided such access, unless otherwise required by law.

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data (except as permitted by Provider's Privacy Policy) to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards. Provider shall only provide access to Student Data to employees or contractors that are performing the Services, except as otherwise permitted in the Service Agreement. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. **[Reserved]**

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service

Agreement, except as necessary to fulfill the purpose of data requests by LEA or as permitted by the Service Agreement.

d. Employee Training. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. Security Technology. When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. Security Coordinator. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. Subprocessors Bound. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding 72 hours. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information to the extent known and practicable:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed because of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached. **ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with an outline copy of said written incident response plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA or required by appliable law. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Joshua Patchak
Title: Executive Director of Technology and Information
Email: jmpatchak@gbaps.org

Contact Information:
Green Bay Area Public School District
200 South Broadway
Green Bay, WI 54303

The designated representative for the Provider for this Agreement is:

Name: Lynn Haaland

Title: Deputy General Counsel, Chief Compliance and Ethics Officer
Email: privacy@zoom.us

Contact Information:
55 Almaden Blvd, San Jose, CA, 95113, Suite 600, USA

b. Notification of Acceptance of General Offer of Privacy Terms. Upon execution of Exhibit "E", General Offer of Privacy Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for notice of acceptance of the General Offer of Privacy Terms is:

Name: Lynn Haaland
Title: Deputy General Counsel, Chief Compliance and Ethics Officer
Email: privacy@zoom.us_____
_____

Contact Information:
55 Almaden Blvd, San Jose, CA, 95113, Suite 600, USA_____

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND

CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF WISCONSIN, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **Successors Bound**. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[*Signature Page Follows*]

DS
AN

IN WITNESS WHEREOF, the parties have executed this Wisconsin Student Data Privacy Agreement as of the last day noted below. Provider:

DocuSigned by:
Lynn Haaland
A6647FCCC21E4B4...

BY: _____ Date: Jul 20, 2020

Lynn Haaland

Printed Name: _____ Title/Position: Deputy GC, Chief Compliance and Ethics Officer

Local Education Agency:

BY: _____ Date: 7/23/2020

Printed Name: Joshua Patchak

Title/Position: Executive Director of Technology and Information

EXHIBIT "A"

DESCRIPTION OF SERVICES

A. **Definitions**. For purposes of this Service Description, the following definitions will apply:

"**Host**" means an individual who is an identified employee, contractor, or agent of Customer to whom Customer assigns the right to host Meetings. A Host may hold an unlimited number of Meetings, but only one Meeting at a time. A Host subscription may not be shared or used by anyone other than the individual assigned to be a Host.

"**Meeting**" means a Zoom Video meeting.

"**Participant**" means an individual, other than the Host, who accesses or uses the Services, with or without the permission and knowledge of the Host.

"**Zoom Documentation**" means this Exhibit, the Zoom website (www.zoom.us) and any additional description of the Services which may be incorporated into this Agreement.

"**Zoom Meeting Services**" means the various video conferencing, web conferencing, webinar, meeting room, screensharing and other collaborative services offered by Zoom Video that Customer may order on an Order Form.

"**Zoom Phone Services**" means voice connectivity services, including, but not limited to, interconnected VoIP services, provisioning of direct dial numbers, and related services offered by Zoom Voice Communications, Inc. ("**Zoom Voice**") that Customer may order on an Order Form.

B. **Zoom Meeting Services**. Zoom Meeting Services enable Hosts to schedule and start Meetings and to allow Participants to join Meetings for the purpose of collaborating using voice, video, and screensharing functionality. Every meeting will have one Host. Chat features allow for out-of-session one-on-one or group collaboration. Further features, functionality, and solutions are described at www.zoom.us.

C. **Zoom Phone Services.** The following sets forth the further terms and conditions that apply to the Zoom Phone Services.

1. **Definitions**: For purposes of the Zoom Phone Services, the following definitions apply:

   "**Device**" means the device assigned to a virtual extension or individual digital line set up within an account or by Zoom at Customer's direction or request.

   "**Phone Host**" means the individual assigned to a number which enables use of the Zoom Voice Service. A Phone Host is a "Host" for purposes of the definition of End User.

   "**Zoom Phone Calling Plan**" means the pricing structure that enables Phone Hosts and End Users to access the PSTN. Calling plans may be "Metered" or "Unlimited" as defined on the Order Form.

   "**Zoom Phone Commitment**" means the minimum monthly bundle of minutes that a Zoom Phone Metered Calling Plan Customer commits to use in connection with Zoom Phone Services.

2. **Telecommunications Provider**. **Zoom Voice is the telecommunications provider of Zoom Phone Services and sets the terms, conditions and rates for Zoom Phone Services.**

3. **Description of Services**. Zoom Phone Services are cloud-based phone services that use voice over internet protocol (**VoIP**) to provide Customer with the following services and functionalities (as selected by Customer on an Order Form):

   a. **Zoom Phone Service**. Zoom Phone Service is a cloud-based phone service that allows two-way voice calling and private branch exchange (PBX) functionality, including, but not limited to, the following features: unlimited extension-to-extension calling (On Net Access), auto attendant/ interactive voice response (IVR), call routing, call queuing, music on hold, call history, caller identification (outbound and inbound), call forwarding, call transfer, and call recording.

   b. **Public Switched Telephone Network Communications (PSTN) Access.** Phone Hosts and End Users can be enabled to make and receive calls to the PSTN and be assigned a direct inward dialing phone number (DID) via a Zoom Phone Calling Plan.

   c. **Bring Your Own Carrier (BYOC).** BYOC allows customers to use the telecommunications provider of their choice to provide PSTN access and inward DID numbers. Zoom provides BYOC customers with software that enables On Net Access and access to a range of Zoom call management features and functions. BYOC enables customers to (i) have PSTN

capability in regions where Zoom does not offer PSTN Access; (ii) maintain relationships with currently deployed carriers; and/or (iii) configure deployments for flexibility and redundancy. Customer must ensure that its carrier provides all regulated telecommunications services and is responsible for telecommunications regulatory compliance.

d. **Additional Zoom Phone Services**. Additional functionality such as enabling common area phones, and additional Toll Free and DID phone numbers may be purchased as described on the Order Form.

4. **Billing and Invoicing.** Zoom will bill Customer on behalf of Zoom Voice based on the Charges set forth on the Order Form. Charges based on usage, or overage amounts that exceed the Zoom Phone Commitment, will be billed in arrears, the month following the month a Charge is incurred. No adjustment will be made, or credit or refund given, for usage that is less than the Zoom Phone Commitment.

   a. **On Net Access**. On Net capability will be provisioned by default for all Zoom Meeting Services. Phone Hosts may access and use On Net services at no charge for so long as the underlying license to the Zoom Meeting Service remains active.

   b. **Taxes**. Customer acknowledges and agrees that Zoom Phone Services are subject to certain Taxes and Fees (including, but not limited to, assessments for universal service) that are not applicable to Zoom Meeting Services. Accordingly, Zoom shall invoice Customer for Taxes and Fees associated with the Charges.

5. **Reasonable Use and Right to Review.** Zoom Voice offers unlimited and metered Phone Calling Plans. These plans are subject to this Zoom Voice Communications, Inc. Reasonable Use Policy. Zoom Phone Calling Plans are for normal and reasonable business use; unreasonable use is prohibited. Use of Zoom Phone may qualify as unreasonable if Customer (a) engages in business activities that involve continual, uninterrupted, or consistently excessive use of Zoom Phone Services, (b) makes any misrepresentations to Zoom Voice that materially affect volume or type of use of Zoom Phone Services, (c) engages in fraudulent or illegal use of Zoom Phone Services, including any activity that violates telemarketing laws or regulations, or (d) uses Zoom Phone Services in any manner that harms Zoom Voice's network or facilities or interferes with the use of the service by other Customers. Use that is inconsistent with the types and levels of usage by typical business customers on the same plan may be used as an indicator of abnormal or unreasonable use, including but not limited to abnormal call lengths; abnormal call frequency; abnormal call duration; abnormal calling patterns that indicate an attempt to evade enforcement of this Zoom Voice Communications, Inc. Reasonable Use Policy. Zoom reserves the right to review Customer use to determine if it is consistent with this Zoom Voice Communications, Inc. Reasonable Use Policy. In the event Zoom Voice determines that You may be engaging in unreasonable use, Zoom Voice will determine the appropriate remedy and will take action to remedy any unreasonable use, including, at its sole discretion, discussing the use with You, moving You to an appropriate Zoom Phone Calling Plan, terminating certain Hosts, and/or otherwise modifying, suspending or terminating Your Zoom Phone services.

6. **Termination of Zoom Meeting Services.** Access to Zoom Phone Services requires a corresponding license to Zoom Meeting Services. In the event that the Zoom Meeting Service license is terminated, the equivalent access to Zoom Phone Services will also be terminated. At such time, Customer will be billed for any incurred usage charges, and will not be credited for any pre-paid amounts toward the Zoom Phone Commitment.

7. **Zoom Voice Policies.** Customer acknowledges and agrees that the Zoom Voice Communications, Inc. policies found at https://zoom.us/legal apply to Customer's use of Zoom Phone Services.

8. **Zoom Emergency Calling (E911) Customer Obligations**. Customer acknowledges and agrees that Customer has read and understood Zoom Voice Communications, Inc.'s 911 Customer Notification, found at www.zoom.us/legal, which sets forth specific limitations of Zoom Phone's emergency calling capabilities and Customer's obligations with respect to its End Users. Such obligations include, but are not limited to:

   a. ensuring that all Phone Hosts receive Zoom Voice's 911 Customer Notification;

   b. ensuring that all assigned phone numbers are registered for emergency calling purposes through the E911 link within Customer's account, and that all registration information remains accurate and up to date; and

   c. distributing warning stickers or other appropriate labels warning End Users that emergency service may be limited or not available and instructing Phone Hosts to place such stickers on or near the Devices and other equipment used in conjunction with Zoom Phone Services.

   Zoom Voice reserves the right at any time to update the Zoom Voice Communications, Inc. 911 Customer Notification as necessary to reflect changes in law or technology that affect the emergency calling capabilities of Zoom Phone Services, and any such updates shall be effective immediately upon Customer's receipt of notice.

9. **Equipment**. Zoom Voice does not supply any Devices or other equipment used in connection with the Zoom Phone Services, and accordingly Zoom Voice does not provide any guarantees as to the quality or operability of such Devices and equipment when used to access Zoom Phone Services. However, Zoom Voice does test certain Devices and equipment to determine whether such Devices and equipment are supported on the Zoom Phone platform (although it has not tested all possible Devices and equipment available in the marketplace). The summary of Devices and equipment to date that Zoom Voice has determined are supported by

the Zoom Phone platform may be provided on request. Customer should consult with Zoom Voice prior to deploying any other Devices and equipment.

D. **Zoom for Government**. Zoom for Government is the Zoom Meeting Services offered by Zoom in a FedRAMP-compliant cloud environment. Zoom for Government enables customers to leverage a limited version of the Zoom Meeting Services in a separate, FedRAMP-compliant cloud environment hosted in Amazon Web Services Government Cloud and Zoom's collocated data centers (e.g. in San Jose, CA and New York), independent of the Zoom's standard commercial cloud environment. Further features, functionality, and solutions are described at www.zoom.us/government. Zoom for Government currently does not include availability of cloud recordings and cloud recording transcriptions, though Zoom may continue to develop feature parity between Zoom Meeting Services and Zoom for Government. In addition, Zoom does not presently offer its Zoom Phone Services or Zoom Marketplace as FedRAMP compliant. Zoom Meeting Services and Zoom for Government are independent environments and, therefore, data cannot be exchanged between them including, without limitation, instant messaging data or chat data.

1. **FedRAMP Security Features.** Zoom for Government is authorized as a FedRAMP Moderate ATO. TLS 1.2 or greater is required. Noted security features include, without limitation, secure socket layer (SSL) encryption, AES 256-bit encryption, role-based user security, watermark screenshots, firewall compatibility, password-protected meeting option. Zoom for Government also supports single sign-on (SSO) with SAML, OAuth, or ADFS.
    i. **Media Data in End-to-End Meeting**. When end-to-end encryption is enabled, all data in transit is protected using TLS 1.2 and AES 256-bit encryption. Data at rest is encrypted leveraging AWS S3 server-side encryption. Zoom web services are secure through HTTPS. In an encrypted meeting, Zoom meeting keys are randomly generated per meeting session. Passwords are hashed/salted using SHA256.
    ii. **Chat/Notes/Closed Captioning in End-to-End Meeting.** When end-to-end encryption is enabled, Chat/Notes/Closed Captioning are transferred with command channel, not data channel; the data travels within SSL connection, and there is no extra AES 256-bit encrypt/decrypt for them.

E. **Zoom Marketplace.** The Zoom Marketplace, available at https://marketplace.zoom.us, is a site hosted by Zoom to provide access to applications (the "Apps") created by third party developers ("Publishers") that are interoperable with Zoom Services, and make them available from both mobile and desktop client apps. Access to and use of the Zoom Marketplace and Zoom for Developers (available at https://developer.zoom.us) sites are governed by separate terms and conditions available at https://zoom.us/service. Besides testing for compatibility with Zoom, Zoom does not perform any other testing and does not warrant or support the Apps. Publishers are solely responsible for all aspects of the Apps they publish, including content, functionality, availability and support. Publishers are required to provide their own terms of service, privacy policy and support information ("Publisher Terms"). Customers who access or download Apps must enter into Publisher Terms directly with the Publisher. Zoom is not responsible for the Apps, their content, functionality, availability, or support. Apps are hosted AS IS and use of the Apps is at Customer's own risk, subject to the Publisher Terms. Apps may become unavailable or be removed by a Publisher at any time and any data stored in them may be lost or become inaccessible. Zoom is not responsible for Customer Data transferred to a Publisher, or for any transmission, collection, disclosure, security, modification, use or deletion of Customer Data by or through an App. Publishers may use Customer Data as permitted in the Publisher Terms. Use of the Apps may require Customer Data to be transferred to the Publisher and by accessing and using the App, Customer consents to the transfer of Customer Data by Zoom as required by the Publisher. Zoom does not support the Apps. Customer should contact the Publisher for support or questions. Zoom makes no representations and disclaims all warranties, express or implied, regarding Apps and reserves the right to remove an App from the Marketplace at any time, in its sole discretion.

F. **Managed Domains**. Zoom permits Customers to reserve domains associated with their enterprise and to manage any accounts that are subscribed to Zoom using that domain ("Managed Domain Customer"). Customer may only associate to the Zoom Services domain(s) that they own or are legally entitled to associate for use with the Services. In the event that a Zoom account is created or exists on the reserved domain, but is not authorized by the Managed Domain Customer (the "Non-Managed Domain Account"), the person using or creating such Non-Managed Domain Account will be notified that the domain is reserved for the Managed Domain Customer and will be requested to change the domain associated with the Non-Managed Domain Account. If the person using or creating such Non-Managed Domain Account does not change the domain within the period specified, that person will be deemed to have consented to the Non-Managed Domain Account being added to the Managed Domain Customer and to have further consented for all data associated with the Non-Managed Domain Account to be shared with the Managed Domain Customer.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used

Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data Please specify:	See Privacy Policy
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken primary language spoken by student)	
	Other demographic information- Please specify:	See Privacy Policy
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information- Please specify:	See Privacy Policy
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	

Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information- Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	X
	Student app username	X
	Student app password	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	X
	Other student work data. Please specify:	See Privacy Policy
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	

	Other transcript data Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data Please specify:	
Other	Please list each additional data element used, stored or collected by your application	See Privacy Policy

OTHER: See Privacy Policy

EXHIBIT "C"

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means all of the following: (1) Any information that directly relates to a pupil that is maintained by LEA;(2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee; and any information that meets the definition of a "pupil record" under Wis. Stat. § 118.125(1)(d). For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School District Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B) and Wis. Stat. § 118.125(2)(d), a School District Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) and Wis. Stat. § 118.125(2) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Wisconsin and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or deidentified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Green Bay Area Public School District directs Zoom Video Communication, Inc. to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

Extent of Disposition Disposition shall be:	Complete. Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	Destruction or deletion of data.
Timing of Disposition Data shall be disposed of by the following date:	As soon as commercially practicable By (Insert Date) _____ [Insert or attach special instructions]

_____ _____
Authorized Representative of LEA Date

_____ _____
Verification of Disposition of Data Date
by Authorized Representative of Provider

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS GREEN BAY AREA PUBLIC SCHOOL DISTRICT

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Green Bay Area Public School District and which is dated to any other LEA ("Subscribing LEA") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Provider:

BY: DocuSigned by: Lynn Haaland A6647FCCC21E4B4... Date: Jul 22, 2020

Printed Name: Lynn Haaland Title/Position: Deputy GC, Chief Compliance and Ethics C

Email Address: Privacy@zoom.us

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Subscribing LEA:

BY:_____ Date:_____

Printed Name:_____ Title/Position:_____

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED ABOVE

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

ZOOM MINIMUM SECURITY CONTROL REQUIREMENTS

These Zoom Minimum Security Control Requirements ("**Minimum Control Requirements**") are stated at a relatively high level. 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 Minimum Control Requirements from time to time. The term "should" in these Minimum Control Requirements 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 Minimum Control Requirements, (i) "**including**" and its derivatives mean "including but not limited to"; (ii) any capitalized terms not defined herein shall have the same meaning as set forth in the Master Subscription Agreement relating to the Services to which these Minimum Control Requirements relate (the "**Agreement**").

1. **DEFINITIONS.**
    1. "**Systems**" means Zoom's production systems.
    2. "**Assets"** means Zoom's production assets.
    3. "**Facilities"** means Zoom's production facilities, whether owned or leased by Zoom (e.g., AWS, data centers).
    4. "**Dependent suppliers**" means Zoom's key vendors/suppliers.

2. **RISK MANAGEMENT.**
    1. **Risk Assessment Program.** The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.
    2. **Risk Assessment.** A risk assessment must be performed annually to verify the implementation of controls that protect business operations and Confidential Information.

3. **SECURITY POLICY.** A documented set of rules and procedures must regulate the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of information and associated services.
    1. **Security Policies and Exception Process.** Security policies must be documented, reviewed, and approved, with management oversight, on a periodic basis, following industry best practices.
        1. 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.
    2. **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.** 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.

1. **Organization**. Current organizational charts representing key management responsibilities for services provided must be maintained.
2. **Background Checks.** Where legally permissible, background checks (including criminal) must be performed on applicable Zoom personnel.
3. **Confidentiality Agreements.** Zoom personnel must be subject to written non-disclosure or confidentiality obligations.

5. **TECHNOLOGY ASSET MANAGEMENT.** 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.

1. **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.
2. **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.
3. Procedures must be in place to remove data from production systems in which Customer Data are stored, processed, or transmitted.

6. **PHYSICAL AND ENVIRONMENTAL.** 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.

1. **Physical and Environmental Security Policy.** Physical and environmental security plans must exist for facilities and scenarios involving access or storage of Customer Data. Additional physical and environmental controls must be required and enforced for applicable facilities, including servers and datacenter locations.
2. **Physical Control.** Storage of Customer Data at new facilities or locations that are not a Zoom facility, as defined herein, must be pre-approved by Customer before use.
3. Physical access, to include visitor access to facilities, must be restricted and all access periodically reviewed.
4. Asset addition/removal process from the production environment must be documented.
5. Policies must be in place to ensure that information is accessed on a need-to-know basis.
6. **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. 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.

1. **Network Identification.** A production network diagram, to include production devices, must be kept current to facilitate analysis and incident response.
2. A current data flow diagram must depict data from origination to endpoint (including data which may be shared with dependent suppliers).
3. **Data Storage.** All Customer Data, including Customer Data shared with dependent suppliers, must be stored and maintained in a manner that allows for its return or secure destruction upon request from Customer.
4. **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.

5. 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.
6. Periodic network vulnerability scans must be performed and any critical vulnerabilities identified must be remediated within a defined and reasonable timeframe.
7. **Clock Synchronization.** Production network devices must have internal clocks synchronized to reliable time sources.
8. **Remote Access.** The data flow in the remote connection must be encrypted and multi-factor authentication must be utilized during the login process.
9. Remote connection settings must limit the ability of remote users to access both initiating network and remote network simultaneously (*i.e.*, no split tunneling).
10. Dependent suppliers' remote access, if any, must adhere to the same controls and must have a valid business justification.
11. **Wireless Access.** Wireless access to the Zoom corporate network must be configured to require authentication and be encrypted.

8. CHANGE MANAGEMENT. 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.

1. **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.
2. 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 post-evaluation of change. Zoom posts service status and scheduled maintenance at https://status.zoom.us.

9. OPERATIONS. Documented operational procedures must ensure 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. 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.

1. **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.
2. **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 processes and be restricted. A periodic review and governance process must be maintained to ensure appropriate provisioning of privileged access.
3. **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 dependent suppliers' environments or when stored by dependent suppliers.

11. DATA INTEGRITY. 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.

1. **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.
2. **Data Transaction Controls.** Controls must be in place to protect the integrity of data transactions at rest and in transit.
3. **Encryption.** Data must be protected and should be encrypted, both in transit and at rest, including when shared with dependent suppliers.
4. **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.
5. **Encryption Uses.** Customer Data must be protected, and should be encrypted, while in transit and at rest. Confidential Information 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. 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.

1. **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. 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.

1. **Business Recovery Plans.** Comprehensive business resiliency plans addressing business interruptions of key resources supporting services, including those provided by dependent suppliers, 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.
2. **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. Zoom must have policies and procedures for back-ups of Customer Data. Back-ups must be protected using industry best practices.

1. **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. Key dependent suppliers must be identified, assessed, managed and monitored. Dependent suppliers 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.

1. **Selection and Oversight.** Zoom must have a process to identify key dependent suppliers providing services to Zoom; these dependent suppliers must be disclosed to Customer and approved to the extent required by the Master Subscription Agreement. Risk assessments of each dependent supplier's control environment must be performed.
2. **Lifecycle Management.** Zoom must establish contracts with dependent suppliers 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 dependent suppliers' fulfillment of contract terms and conditions.

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

1. **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.
2. **System Patches.** Security patch process and procedures, to include requirements for timely patch application, must be documented.
3. **Operating System.** Versions of operating systems in use must be supported and respective security baselines documented.
4. **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. 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 Data are monitored, controlled and protected.

1. **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.
2. Application layer controls must provide the ability to filter the source of malicious traffic.
3. Restrictions must also be placed on or in front of web server resources to limit denial of service (DoS) attacks.
4. Zoom must monitor uptime on a hosted web or mobile application.
5. **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 development of secure software, for example:
    - Security requirements in requirements phase,
    - Secure architecture design,
    - Static code analysis during development,
    - Dynamic scanning or penetration testing of code during QA phase.

1. Validation of security requirements must follow a documented methodology.
2. SDLC methodology must include requirements for documentation and be managed by appropriate access controls. Developer access to production environments must be restricted by policy and in implementation.
3. Code certification, including security review of code developed by third parties (*e.g.*, open source, contracted developers), must be performed. Third-party and open source code used in applications must be appropriately licensed, inventoried, supported, patches applied timely, tested prior to use in production, and evaluated for security defects on an on-going basis, with any identified gaps remediated in a timely manner.

7. Testing and Remediation. Software executables related to client/server architecture that are involved in handling Customer Data must undergo vulnerability assessments (both the client and server components) 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.

1. 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.

8. Zoom must conduct penetration testing on an annual basis.

18. VULNERABILITY MONITORING. 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.

1. **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 Data.
2. **Malware.** In production, Zoom must employ tools to detect, log and disposition malware.
3. **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 real-time alerting. IDS/advanced threat protection signatures must be kept up-to-date to respond to threats.
4. **Logging and Event Correlation.** Monitoring and logging must support 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.

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

1. **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.
2. **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.
3. **Business Continuity Management and Operational Resiliency.** Business continuity plans to meet recovery time objectives (RTO) and recovery point objectives (RPO) must be in place.
4. **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.

5. **Encryption and Key Management.** All communications must be encrypted in-transit between environments.
6. **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.
7. **Identity and Access Management.** Management of accounts, including accounts with privileged access, must prevent unauthorized access and mitigate the impacts thereof.
8. **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.
9. **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 dependent suppliers.
10. **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. 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.

1. 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, 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.