Zoom Video Communications, Inc.
Information Security Addendum

This Information Security Addendum ("**Addendum**") is effective as of the last date signed below ("Addendum Effective Date") and is entered into by and between _____, ("**Vendor**") and Zoom Video Communications, Inc. ("**Zoom**"). Vendor and Zoom shall be referenced in this Addendum each as a **"Party"** and, together, as the **"Parties."**

RECITALS

WHEREAS, the Parties have or will enter into one or more separate agreement(s) for the provision of goods, software and/or services to Zoom pursuant to which Vendor may access Zoom Data and/or Zoom Systems ("**Agreement**");

WHEREAS, the Parties intend for this Addendum to operate as supplemental to any Agreement between the Parties and any such Agreement shall not be deemed to modify or supersede the terms of this Addendum, unless such Agreement expressly references this Addendum and the terms it intends to modify or supersede, or the conflicting terms in the Agreement provide more rigorous protection;

NOW, THEREFORE, in consideration of the promises set forth herein, the Parties agree as follows.

AGREEMENT

I. Definitions. Capitalized terms used, but not otherwise defined, in this Addendum will have the meanings given them in the Agreement.

A. "Media" means optical, magnetic, or other media of Vendor used to store Zoom Data.

B. "Personal Data" means any information that Vendor receives from or on behalf of Zoom, when such information identifies, is identifiable to, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular Data Subject or the household of a Data Subject.

C. "Personnel" means Vendor's employees, contractors, subcontractors, and agents.

D. "**Products**" means any hardware, software, cloud services, or deliverables furnished by Vendor under the Agreement.

E. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, acquisition, modification, or destruction of Zoom Data or interference with the operations or integrity of Zoom Systems or products.

F. "Services" means any professional or other services rendered by Vendor under the Agreement.

G. "**Systems**" means a Party's computers, networks, servers, software, and electronic communications systems, including but not limited to voicemail, email, databases, and internet and intranet systems.

H. "**Zoom Data**" refers to information, data, or content of any kind whether in the form of copy, text, images, video, audio files or other form, and regardless of the format, including all logos, proprietary marks, distribution lists, URLs or other information, data or content supplied or made available by or on behalf of Zoom or its customers, and all information created or generated in the course of using a Service, including all intellectual property rights contained therein. Zoom Data includes Personal Data.

II. Representations and Warranties. Vendor represents and warrants that it maintains physical, technical, and administrative safeguards designed to maintain the confidentiality, integrity, and availability of the Zoom Data and Zoom Systems involved in Vendor's provision of Products and Services, and to prevent unauthorized access, intrusion, alteration, or other interference of the same. Such safeguards shall be no less rigorous than those maintained by Vendor for its own or other customers' data and must comply with

(i) the requirements of this Addendum; (ii) applicable laws and regulations; and (iii) industry best practices (unless such practices conflict with this Addendum). Vendor further represents and warrants that Vendor and its Personnel will only use Zoom Data and Zoom Systems solely for Zoom's benefit and exclusively for the purposes authorized by Zoom in the Agreement and this Addendum.

III. Independent Security Controls Assessment. Vendor has and will maintain an independent third party certification or attestation of the controls to safeguard the confidentiality, integrity, and availability of Zoom Data on at least an annual basis (e.g., SOC 2 Type II, ISO 27001, HITRUST, PCI-DSS, etc.). Upon request, Vendor will provide evidence of the completed attestation/certification and report, including findings, recommendations, and remediation plans or evidence that the findings have already been remediated. Unremediated material findings will be subject to Section IX(A).

IV. Information Security Program. Vendor must maintain a formalized and documented information security program. At a minimum, Vendor's information security program and associated controls must meet the following requirements:

A. Information Security Policy and Standards. Vendor adheres to written information security policies and standards ("**Security Policies and Standards**"), which address the roles and responsibilities of its Personnel, set forth the minimum safeguards for the protection of Zoom Data, and are reviewed and updated at least annually and when there is a material change in business practices that may reasonably impact Zoom Data, Zoom Systems, and/or the Products/Services. The Security Policies and Standards must set forth physical, technical, and administrative safeguards that are appropriate for Vendor's on-premises assets, cloud/virtual environments, size, and Products and/or Service, as well as for the volume and sensitivity of the data that Vendor processes.

B. Access Controls. Vendor shall maintain physical and logical system access provisioning processes that meet or exceed industry standards for all Vendor Systems that access, process, or store Zoom Data or Zoom Systems, including provisioning access thereto based on the principle of least privilege.

1. **Physical Access.** All Zoom Data will be stored in secured data centers ("**Secured Areas**") with physical and environmental safeguards appropriate to the risk exposure. Vendor will maintain and regularly audit a list of authorized Personnel.

2. **Logical Access.** Vendor's processes must include timely access terminations, regular reviews of access provisioning, and audits of access to Zoom Data and Zoom Systems as needed and at a regular cadence appropriate to the risk exposure.

3. **Authentication.** Multi-factor authentication must be in place on all Vendor Systems that access, store, process, or transmit Zoom Data or Zoom Systems. Where password authentication is employed to authenticate Personnel, Vendor will meet or exceed the standards provided by NIST 800-63 or equivalent.

C. Computing and Network Infrastructure Controls. Network segments where Zoom Data resides will be physically or logically isolated from segments containing other data. Firewalls must be in place on all egress and ingress points of networks on which Zoom Data is stored or processed and changes made to firewall rule sets or other network infrastructure must be managed by a change control system.

D. Data Loss Prevention ("DLP"). Vendor will employ a DLP solution with related monitoring and response procedures that meets or exceeds industry standards to block the unauthorized export of Zoom Data outside Vendor's network.

E. Intrusion Detection and Prevention. Vendor will employ and actively monitor network intrusion detection and intrusion prevention tools on a twenty-four (24) hours a day, seven (7) days a week basis with a maximum reaction time of no more than forty-eight (48) hours for real or suspected Security Incidents.

F. Monitoring and Logging. Vendor must maintain a process that meets or exceeds industry standards for the monitoring and detection of potential Security Incidents. Vendor must maintain event logs reasonably designed to enable investigation of actual and potential Security Incidents. Vendor must review relevant event logs on a routine and as-needed basis for unauthorized access or misuse, and take necessary actions in response to anomalous activity.

G. Disposal of Files, Media, or Products Containing Zoom Data. For any Media or Products containing Zoom Data that must be destroyed, Vendor must do so securely in accordance with NIST 800-88 and be able to provide a certificate of destruction upon Zoom's request.

H. External Access.

1. **Internet.** Vendor will implement a comprehensive "defense in depth" network architecture and process that includes industry standard architecture, tools, and practices.

2. **Remote Access.** If Personnel remotely access from offsite locations Vendor Systems and Media that process Zoom Data, Vendor will maintain industry standard safeguards, Systems, and procedures to secure such connections and transmissions.

I. Restrictions on Uses of Portable Devices or Media. Zoom Data may only be accessed, transmitted, used, stored, or processed on Vendor managed applications and devices, and any such portable devices must be encrypted in accordance with Section IV.O.

J. Malware Controls. Vendor will employ up-to-date virus, anti-malware, and other commercially reasonable system security agents on Vendor Systems and Media, and such protection tools will include real-time or regular scans for viruses.

K. Patch Management. Vendor shall implement and maintain patch management procedures that meet or exceed industry standards and that require patches to be prioritized, tested, and installed based upon criticality for all Systems accessing, storing, transmitting and/or processing Zoom Data. Criticality will be assessed using the NVD Vulnerability Severity Ratings based on the Common Vulnerability Scoring System (CVSS) v3.0 base score ranges (adjusted, as needed, by temporal and environmental scores). Vendor will remediate "critical" and "high" vulnerabilities within thirty (30) days, "medium" vulnerabilities within ninety (90) days, and "low" vulnerabilities within 120 days. Vendor shall maintain change logs that document patch implementation activities.

L. Security Training and Awareness.** Vendor will ensure that all Personnel who will have access to Zoom Data or to Systems or Media processing Zoom Data will undergo information security training upon hire, prior to being granted access to Zoom Data, and at least annually thereafter.

M. Information Security Incident Management. Vendor will maintain and test at least annually, an information security incident response plan, which will be provided to Zoom upon request. Such plan must set forth processes for the intake, investigation, and resolution of actual and reasonably suspected Security Incidents, including severity rating to prioritize alerts and incidents for response by a dedicated incident response team. In the event of an actual or reasonably suspected Security Incident impacting Zoom Data, Vendor will: (1) Notify Zoom at tprm@zoom.us within twenty-four (24) hours of discovery of any Security Incident; and (2) Provide regular status updates and assist Zoom as needed for Zoom's compliance with any investigation, notice, or reporting requirements.Vendor will provide Zoom with a final written report no later than fifteen (15) days following the closure of such incident, detailing the root cause of the incident, the actions taken, the impact to Zoom, and remediation measures planned to prevent future occurrences.

N. Penetration Test. Vendor will have a penetration test of its entire environment (including Vendor Systems, web services, Products, configurations, and corporate/production/development environments, as applicable) performed at least annually by a qualified third party firm that includes, but is not limited to, testing for OWASP top 10 vulnerabilities (as applicable). Upon request, Vendor will provide an executive summary of the penetration test results, including findings, recommendations, and

remediation plans or evidence that the findings have already been remediated. Unremediated material findings will be subject to Section IX(A).

O. Encryption. Zoom Data must be encrypted using industry standard encryption at rest (e.g., AES-256) and while in transit (e.g., TLS 1.2) over public networks; Zoom Data must be encrypted while in transit over non-public networks or similarly protected using compensating controls. Authentication credentials must be encrypted in transit and salted and hashed in storage, and Vendor will maintain a key management process that meets or exceeds industry standards for each component of the key management lifecycle.

P. Wireless Devices. Vendor's wireless network must be configured to require authentication, be encrypted, and must otherwise be implemented to meet or exceed industry standards.Vendor will maintain a process to detect rogue access points at least quarterly to ensure that only authorized wireless access points are in place.

Q. IoT Detection and Assessment. At least quarterly, Vendor will maintain a program to detect and evaluate Internet of Things (IoT) devices (e.g., Smart HVAC, wireless backup devices, automation devices, etc.) for compliance with Vendor's security program.

R. Device Hardening. Vendor will maintain a process that meets or exceeds industry best practices for system hardening, including, but not limited to, prohibiting the use of default passwords.

S. Third Party Information Security Requirements. For all third parties engaged by Vendor that store, process, or transmit Zoom Data (or that access Vendor Systems on which Zoom Data is stored, processed, or transmitted), including contractors and agents, Vendor will ensure that such third parties adhere to standards that materially meet or exceed the requirements set forth in this Addendum.

T. Employee Records Checks. For Personnel who will have access to Zoom Data, Zoom Systems, or Systems or areas in which Zoom Data is processed or stored, Vendor will perform local, state, and national agency records checks covering a minimum of seven (7) years for criminal activity; education verification; and prior employment verification. Subject to applicable law, individuals with felony or misdemeanor convictions for theft, fraud, or drug use, will not be allowed to work on the Zoom account or have access to Zoom Data, Zoom Systems, or Systems areas in which Zoom Data is processed or stored.

U. Business Continuity Management. Vendor must have an enterprise business resilience/business continuity program to assure the timely and orderly recovery of business, support processes, operations, and technology components. Vendor agrees to restore Services with a Recovery Time Objective (RTO) of __ hours and a Recovery Point Objective (RPO) of __ hours. The business continuity program requirements below must be documented, tested, reviewed, and approved with management oversight on at least an annual basis:

1. **Business Impact Analysis.** Vendor will conduct a business impact analysis for all Vendor Systems and Media, including those provided by subprocessors, related to the provision of Vendor's Products/Services to identify key business functions and resources.

2. **Business Recovery Plans.** Vendor will maintain business recovery plans setting forth the resources and actions required to minimize disruption to Vendor's Products/Services. The business resiliency plan must have an acceptable alternative work location in place to ensure service level commitments are met.

3. **Technology Recovery Plans.** Vendor will maintain technology recovery plans setting forth the resources and actions required to minimize Service interruptions and ensure recovery of Vendor Systems.

V. Right to Audit. In addition to any other audit rights set forth in this Addendum and the Agreement, Zoom and its authorized agents will have the right to audit Vendor's information security program annually (or as

otherwise reasonably agreed by the Parties) within thirty (30) days written notice for compliance with this Agreement, this Addendum, and applicable laws, rules, and regulations. Vendor will provide all such cooperation as may be reasonably requested by Zoom to perform the audit.

A. If applicable, Zoom or a third party firm on its behalf will be permitted to penetration test Vendor's Systems and/or Products subject to mutually agreeable terms.

B. As part of the audit, Vendor will be subject to review by security rating sites or businesses.

C. Zoom will provide Vendor with a report of material findings and recommendations. Vendor will provide Zoom with remediation plans or evidence that the findings have already been remediated. Unremediated material findings will be subject to Section IX(A).

VI. **Notifications; Control.** If a Security Incident caused by Vendor or its agents, contractors, or subprocessors requires notification by or on behalf of an individual or regulator under any law or regulation, Zoom will have sole control over the timing, content, and method of notification and Vendor will promptly reimburse Zoom for all costs and expenses incurred as a result of the breach, including but not limited to, notice, print, mailing, call center costs, and the costs of obtaining two years of credit monitoring services and identity theft insurance for the individuals whose data was or may have been compromised.

VII. **Communication Systems and Access to Information.** During the term of the Agreement, Vendor may receive access to Zoom Systems. Such Systems are intended for legitimate business use related to Zoom's business. Vendor acknowledges that Vendor does not have any expectation of privacy as between Vendor and Zoom in the use of or access to Zoom's Systems and that all communications made with the Zoom Systems or equipment by or on behalf of Vendor are subject to Zoom's scrutiny, use, and disclosure, in Zoom's discretion. Zoom reserves the right, for business purposes, to monitor, review, audit, intercept, access, archive, and/or disclose materials sent over, received by or from, or stored in any of the Zoom Systems. Zoom reserves the right to override any security passwords to obtain access to voicemail, email, computer (and software or other applications) and/or computer disks on and Zoom System. Vendor also acknowledges that Zoom reserves the right, for any business purposes, to search all work areas (e.g., offices, cubicles, desks, drawers, cabinets, computers, computer disks, and files) and all personal items brought onto Zoom property or used to access Zoom Data or Zoom System.

VIII. **Regulatory Compliance**. In the event Vendor's relationship with Zoom under this Agreement is identified in writing by any regulator having jurisdiction over Zoom to present a material risk to Zoom or its business partners or customers that requires correction, Zoom will notify Vendor of such identification. The Parties will use reasonable efforts to resolve the identified issue(s) to the satisfaction of the relevant regulator within the timeframe mandated by the regulator; issues that are not so resolved will be subject to Section IX(A).

IX. Term/**Termination.** This Addendum will continue in force until otherwise terminated in accordance with this Section. Either Party may terminate this Addendum upon thirty (30) days written notice if there are no outstanding Orders and Vendor no longer has access to Zoom Data and/or Zoom Systems.

A. This Section IX(A) applies to provisions where expressly stated. If material findings or issues are not remediated or resolved to Zoom's satisfaction, Zoom will have the right to terminate the Agreement for convenience on thirty (30) days written notice, without liability for any termination fees or penalties or any costs, fees, or expenses not incurred up through the effective date of termination. Upon termination, Vendor will be required to complete Zoom's offboarding process.

X. **Application Security for Products.** In addition to the requirements above, Products must also adhere to the following:

A. **Software Development Life Cycle.** Vendor must maintain a Software Development Life Cycle (SDLC) policy and process by which Personnel create secure Products and Services, and which sets forth the required activities at each stage of development (requirements, design, implementation, verification, documentation, and delivery), including release management procedures, which meet or

exceed industry standards and are regularly documented, reviewed, approved, and version-controlled, with management oversight.

B. Secure Development. The SDLC shall follow secure application development policies and procedures that are aligned to industry-standard practices, such as the OWASP Top 10. Without Zoom's written approval, no Products will contain any "phone-home," metering, or other features designed to periodically transmit usage, statistical, or other data to Vendor or any third party. Vendor will ensure that (i) Open Source Software furnished to Zoom will not contain orphaned code, and (ii) no Products or any component thereof contain any hardware or software that is end-of-life or unsupported.

C. Testing and Remediation. Software executables related to client/server architecture that are involved in handling Zoom Data must undergo vulnerability assessments that meet or exceed industry standards (both the client and server components) prior to release and on an on-going basis, and any gaps identified must be prioritized, tested, and remediated based upon criticality. Criticality will be assessed using the NVD Vulnerability Severity Ratings based on the Common Vulnerability Scoring System (CVSS) v3.0 base score ranges (adjusted, as needed, by temporal and environmental scores). Vendor will remediate "critical" and "high" vulnerabilities within thirty (30) days, "medium" vulnerabilities within ninety (90) days, and "low" vulnerabilities within 120 days. 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, and must include a vulnerability scan encompassing all ports and fuzz testing, static code analysis tools, and an anti-virus scan, with up to date signatures.

D. Change Management. Vendor will maintain a change management program for the Products, that includes logically or physically separate environments from production for all development and testing. No Zoom Data will be transmitted, stored, or processed in a non-production environment.

E. Bug Bounty. Vendors must: (a) have a bug bounty program ("BBP") or vulnerability/responsible disclosure program ("VDP"); or (b) allow Zoom to include the Product/Service and/or domain in scope for Zoom's BBP.

For vulnerabilities that: (a) originate in Vendor's Systems and/or Products/Services; (b) have the potential to materially impact the security of Zoom Data, Zoom Systems, and/or Zoom products; and (c) are reported to Vendor's BBP/VDP or Zoom's BBP/VDP:

1. Vendor shall remediate reported vulnerabilities in accordance with Sections IV.K. and X.C. (as applicable).

2. If Vendor cannot fix critical and high severity vulnerabilities in accordance with Sections IV.K. or X.C. (as applicable), Vendor shall promptly notify Zoom and provide a description of the vulnerability, the reasons why the vulnerability cannot be remediated within the agreed time frame, the proposed remediation plan and timeline, and facts sufficient for Zoom to evaluate the potential impact and risk to Zoom; such vulnerabilities will be subject to Section IX(A).

   If vulnerabilities originating in Vendor's Systems or Products/Services are reported to Zoom's BBP, Zoom will notify Vendor of the reported vulnerability as soon as is practicable and Vendor will reimburse Zoom for all resulting bounties up to $50,000 per bounty that are paid in accordance with Zoom's BBP (the terms of which may be subject to change).

3. Vendor shall not (nor shall it allow security researchers to) directly or indirectly refer to Zoom without Zoom's written consent in any public disclosures regarding vulnerabilities reported to Vendor's BBP/VDP or Zoom's BBP/VDP.

F. Website Security. Vendors that host Zoom's externally facing websites must make reasonable efforts to ensure that common website threats/attacks are mitigated, including, but not limited to:

1. **Cross-Site Scripting (XSS).** Vendor will remove or disable markup that can potentially contain instructions for attackers to inject client-side scripts through the website into the user's browsers (e.g., for HTML this includes elements, such as <script>, <object>, <embed>, and <link>).

2. **SQL Injection.** Vendor will ensure that any user data passed into an SQL query cannot change the nature of the query to prevent malicious users from executing arbitrary SQL code on a database (e.g., escape all the characters in the user input that have a special meaning in SQL).

3. **Cross-Site Request Forgery (CSRF).** Vendor will ensure that servers require that POST requests include a user-specific site-generated secret, supplied by the server, when sending web form requests to minimize malicious users executing actions using the credentials of another user without that user's knowledge or consent.

4. **Clickjacking.** Vendor will ensure appropriate HTTP headers are set to prevent and ensure websites are not embedded in an iframe in another site, reducing the risk of a malicious user hijacking clicks and routing them to a hidden page beneath or unwittingly clicking a completely different button.

5. **Denial of Service (DoS).** Vendor will implement measures before or in the webserver to identify and block "bad" traffic while allowing legitimate messages through to prevent the flooding of a target site with fake requests, disrupting access to the site for legitimate users.

6. **Directory Traversal, File Inclusion, and Command Injection.** Vendor will sanitize user input prior to the data being used to help prevent these common attacks/vulnerabilities.

Except to the extent specifically modified herein, all other provisions of the Agreement shall remain in full force and effect. In the event of a conflict between this Addendum, the Agreement, and/or any other terms and conditions entered into between the Parties (e.g., a Business Associate Agreement, a Data Processing Addendum, etc.), the provision providing the most rigorous protection will take precedence.

VENDOR: **[INSERT VENDOR NAME]** By: _____ *(Signature)* Name: _____ *(Print)* Title: _____ Date: _____	Address for notices: _____ _____ _____ _____ Phone: _____ Fax: _____
Zoom: **Zoom Video Communications, Inc.** By: _____ *(Signature)* Name: _____ *(Print)*	Address for notices: _____ _____ _____ _____

Title: _____	Phone: _____
Date: _____	Fax: _____