Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: Universität Paderborn

Address: Warburger Straße 100, 33098 Paderborn, Germany

Tel.: [redacted]; fax: ; e-mail: [redacted]

Other information needed to identify the organisation:

And

Name of the data importing organisation: Zoom Video Communications, Inc.

Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113

[redacted]

Other information needed to identify the organisation: not applicable

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '*personal data*', '*special categories of data*', '*process/processing*', '*controller*', '*processor*', '*data subject*' and '*supervisory authority*' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) '*the data importer*' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC Processor;

(d) '*the subprocessor*' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) '*technical and organizational security measures*' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has

to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the

data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer

under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): ...[redacted].....

Position: [redacted].

Address: .....Universität Paderborn, Warburger Straße 100, 33098 Paderborn, Germany.....

Other information necessary in order for the contract to be binding (if any):

Signature [redacted]

(stamp of organization)

On behalf of the data importer:

Name (written out in full): [redacted]

Position: [redacted]

Address: 55 Almaden Blvd, Suite 600, San Jose, CA 95113. USA

Other information necessary in order for the contract to be binding (if any): not applicable

DocuSigned by:

Signature.....[redacted].....

(stamp of organization)

1 This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is a customer or other user of the data importer's communication software, services, systems and/or technologies.

Data importer
The data importer is a provider of communication software, services, systems and/or technologies.

Data subjects
Individuals about whom data is provided to Processor via the Services by (or at the direction of) Controller or Controller's end users, including without limitation Controller's employees, consultants, contractors, agents, and end users

Categories of data
Any Personal Data provided to Zoom via the Services, by (or at the direction of) Customer or Customer's end users, including but not limited to the following:

Cloud Recordings (optional): Mp4 of all video, audio and presentations, M4A of all Audio, Text file of all in meeting chats, Audio transcript file

IM Chat Logs

Special categories of data (if appropriate)
Special categories of data are not required to use the service. The data exporter may submit special categories of data to Customer, the extent of which is determined and controlled by the data exporter in its sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.

Processing operations
The personal data transferred may be subject to the following basic processing activities:

- account configuration and maintenance;
- facilitating conferences and meetings between data subjects and third-party participants;
- hosting and storing personal data arising from such conferences and meetings solely for the purposes of providing the services;
- customer/ client technical and operational support

DATA EXPORTER

Name: .....Universität Paderborn.....

Authorised Signature: [redacted]

DATA IMPORTER

Name: Zoom Video Communications, Inc.

Authorised Signature: DocuSigned by: [redacted]

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see **EXHIBIT B** for a description of Zoom's Security Measures.

DATA EXPORTER

Name: Universität Paderborn

Authorised Signature: [redacted]

DATA IMPORTER

Name: Zoom Video Communications, Inc.

Authorised Signature: DocuSigned by: [redacted]

EXHIBIT B

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.
        - 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 appropriatelyrobust 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.

a) Validation of security requirements must follow a documented methodology.
b) 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.
c) 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.

6. **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.
   a) Testing must be based on, at a minimum, the OWASP Top 10 risks (or the OWASP Mobile Top 10 risks, where applicable), or comparable replacement.
   b) Zoom must conduct penetration testing on an annual basis.

18. **VULNERABILITY MONITORING.** 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. 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.