DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") applies to the agreement, including any order forms or other similar purchasing documents, between Data Controller ("Customer") and Netskope, Inc., by and on behalf of its Affiliates ("Netskope") governing the provision of Netskope services purchased by Customer ("Services"), under which Netskope Processes certain Personal Data as part of performing thereunder (collectively, the "Agreement"), and reflects the parties' agreement related to Processing of Customer Data, including Personal Data, in accordance with applicable Data Protection Requirements.

HOW TO EXECUTE THIS DPA

1. This DPA consists of two parts: the main body of the DPA including Appendix 1 & 2 and Schedule 1 relating to the Standard Contractual Clauses.
2. To complete this DPA, Customer must
   a. complete the Controller information in the signature box and sign on Page 6.
   b. complete the SCC section on page 11, 17, 18 and sign page 16
   c. Send the completed and signed DPA to Netskope by email to privacy@netskope.com.

Upon receipt of the completed DPA by Netskope, Inc. at this email address, this DPA will become legally binding with respect to Services provided.

HOW THIS DPA APPLIES

This DPA shall not replace any rights related to Processing of Customer Data previously negotiated by Customer in the Agreement but shall replace any existing data processing addendum to the Agreement, unless otherwise explicitly stated herein.

DATA PROCESSING TERMS

In the course of providing the Services to Customer pursuant to the Agreement, Netskope may Process Personal Data on behalf of Customer. Netskope agrees to comply with the following provisions with respect to any Personal Data collected and Processed by or for Customer using the Services.

1. DEFINITIONS

1.1. "**Affiliate**" means any present or future entity controlling, controlled by, or under common control with, a Party.

1.2. "**Customer Data**" means all data or information submitted by or on behalf of Customer or its Affiliates to the Services, as well as the output of the Services as a result of Processing such data or information for Customer.

1.3. "**Data Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.4. "**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.

1.5. "**Data Protection Requirements**" means all data protection and privacy laws and regulations, as applicable to a party, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; and (ii) any other local or regional data protection, data privacy or data security laws. It also includes, where applicable to Netskope's business, in its delivery of the Services, or as otherwise required in this DPA, application of certain certification requirements, specifically both the EU-U.S. and Swiss-U.S. Privacy Shield Principles, as further described in this DPA.

1.6. "**Data Subject**" means an identified or identifiable natural person whose Personal Data is collected and hosted by Netskope in connection with the Services, as may be more fully set forth in Data Protection Requirements and shall be meant to include any different but similar term used in Data Protection Requirements.

1.7. "**EEA**" means the European Economic Area and includes member states of the European Union as well as Iceland, Liechtenstein and Norway.

1.8. "**GDPR**" means the General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.9. "**Personal Data**" means any information relating to an identified or identifiable natural person as further defined under Data Protection Requirements, which may include a term similar to Personal Data but which shall have the same general meaning (for example "personal information"), where such information is Customer Data as further specified in Appendix 2.

1.10. "**Privacy Shield**" means the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield self-certification programs, both operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of July 12, 2016 (and as may be amended from time to time) and pursuant to the Swiss Federal Council pronouncement on 11 January 2017.

1.11. "**Privacy Shield Principles**" means the Privacy Shield Framework Principles (as supplemented by any Supplemental Principles) which may be found on the U.S. Department of Commerce website, and as may be amended, superseded or replaced from time to time.

1.12. "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, shall be meant to include any different but similar term used in the Data Protection Requirements and as may be more fully set out in Appendix 2.

1.13. "**Restricted Transfer**" means a transfer of Personal Data by Netskope to a jurisdiction outside of the European Union, unless the transfer is made (a) to an Adequate Jurisdiction (as permitted by the GDPR), or (b) pursuant to a data transfer mechanism permitted under the GDPR, or (c) pursuant to a lawful exemption or derogation under the GDPR.

1.14. "**Security Specifications**" means the security measures employed by Netskope to protect the Personal Data in its possession in connection with delivering the Services, which will include the requirements set forth in Appendix 1.

1.15. "**Standard Contractual Clauses**" means the set of standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council as may be updated or otherwise amended.

1.16. "**Sub-processor**" means any Data Processor engaged by Netskope used to deliver the Services.

Any capitalized terms not otherwise defined within this DPA shall have the meaning given to them in the Agreement or applicable Data Protection Requirements.

2. PROCESSING OF PERSONAL DATA

2.1. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller, Netskope is a Data Processor and that Netskope will engage Sub-processors pursuant to the requirements set forth in Section 5 ("Sub-processors"). Further, each Party agrees to comply with its respective obligations under the Data Protection Requirements in relation to its Processing of the Personal Data and Netskope agrees to provide assistance reasonably required by Customer to enable Customer to take reasonable and appropriate steps to ensure that Netskope effectively Processes Personal Data in a manner consistent with Customer's obligations under Data Protection Requirements, including the GDPR or the Privacy Shield Principles, as applicable.

2.2. **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Requirements. Customer will ensure that its instructions to Netskope, for the Processing of Personal Data, shall comply with the Data Protection Requirements; Customer remains responsible for selecting appropriate Service options and configurations for Customer's compliance requirements.

2.3. **Netskope Processing of Personal Data**. Netskope shall only Process Personal Data on behalf of and in accordance with Customer's instructions. Customer instructs Netskope to Process Personal Data for the following purposes: (i) Processing to provide the Services in accordance with the Agreement and applicable Service order(s); (ii) Processing initiated by designated and authorized Customer representatives in their use of the Services; and (iii) Processing to comply with other reasonable instructions by Customer that are consistent with the terms of the Agreement. Further, Netskope agrees that it shall, in its capacity as Data Processor:

2.3.1. Only carry out Processing of Personal Data on Customer's instructions, as set forth in the Agreement and this DPA, for the purpose of providing the Services;

2.3.2. Provide at least the same level of protection to Personal Data as is required by this DPA and the Data Protection Requirements;

2.3.3. Promptly notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by Data Protection Requirements, and in such event, to work with Customer to promptly take reasonable and appropriate steps to stop and remediate any Processing until such time as the Processing meets the level of protection as is required by the Data Protection Requirements;

2.3.4. Implement and maintain throughout the term of this DPA appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and accidental destruction or loss (including ensuring the reliability of employees), so as to allow Customer to comply with the requirement to implement appropriate technical and organizational security measures, in accordance with the Security Specifications and other applicable provisions of the Data Protection Requirements;

2.3.5. At Customer's sole election, to cease Processing Personal Data promptly if in Customer's reasonable discretion, Netskope is not providing the same level of protection to Personal Data as is required by Data Protection Requirements.

2.3.6. Keep or cause to be kept full and accurate records relating to all Processing of Personal Data on behalf of Customer as part of the Services ("Records");

2.3.7. Promptly refer to Customer any requests, notices or other communication from Data Subjects, any national data protection authority established in the jurisdiction of Customer, or any other law enforcement authority, for Customer to resolve;

2.3.8. Provide assistance reasonably required by Customer to enable Customer to respond to, comply with or otherwise resolve any request, question or complaint made to it by a Data Subject in relation to the Processing of Personal Data associated with such Data Subject;

2.3.9. Provide assistance reasonably required by Customer to enable Customer to respond to, comply with or otherwise resolve any request, question or complaint made to it that is received from: (a) any independent recourse mechanism that Customer elects to adopt under the Privacy Shield Principles (where applicable); (b) any applicable U.S., EU or Swiss regulator or data protection authority; or (c) any arbitration panel set up under Annex I to the Privacy Shield Framework.

2.3.10. Take reasonable steps to ensure the reliability of any of its employees who have access to the Personal Data.

2.3.11. Netskope agrees it will not, in its capacity as Data Processor:

2.3.11.1. Disclose Personal Data to any third party individual other than for the purpose of complying with Data Subject access requests in accordance with Data Protection Requirements and in accordance with Sections 2.3.8 to 2.3.10, as applicable.

2.3.11.2. Include Personal Data in any product or service offered by Netskope to third parties;

2.3.11.3. Share or allow access to files containing Personal Data to any third party for further Processing by that third party or its agents, excluding third parties used merely for routing Personal Data, such as routing through a telecommunications carrier and excluding those Sub-Processors approved by Customer pursuant to Section 5.1 or as otherwise approved within the Agreement.

Netskope's obligations as set forth in Sections 2.3.4, 2.3.6 through 2.3.11 shall survive termination until such time Netskope no longer Processes Personal Data.

3. RIGHTS OF DATA SUBJECTS

3.1. Correction, Blocking and Deletion. To the extent Customer, in its use of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Requirements, Netskope shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Netskope is legally permitted to do so. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Netskope's provision of such assistance.

3.2. Data Subject Requests. Netskope shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of that individual's Personal Data. Netskope shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request has been received and relates to Customer. Netskope shall provide Customer with commercially reasonable cooperation and assistance in relation to a Data Subject's request for access to that individual's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use of the Services. If legally permitted, Customer shall be responsible for any reasonable costs arising from Netskope's provision of such assistance.

4. NETSKOPE PERSONNEL

4.1. Reliability. Netskope shall take commercially reasonable steps to ensure the reliability of any Netskope personnel engaged in the Processing of Personal Data.

4.2. Limitation of Access. Netskope shall ensure that access to Personal Data by its personnel is limited to those who require such access to perform under the Agreement.

4.3. Privacy Representative. Netskope has appointed a privacy representative to respond and address requests relating to Personal Data. The privacy representative may be reached at privacy@netskope.com Where required by Data Protection Requirements, Netskope Affiliates may also appoint a data protection officer who can be reached at the same address.

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that Netskope may engage third-party Sub-processors in connection with the provision of the Services. Netskope will enter into contractual terms with each Sub-processor consistent with the requirements of this DPA, as necessary for compliance with Data Protection Requirements based upon the nature of the service provided by the Sub-processor, which shall at a minimum require the Sub-processor to agree to (a) act only on Netskope's instructions in Processing the Personal Data (which instructions shall be consistent with Customer's instructions to Netskope), and (b) protect the Personal Data to a standard consistent with the requirements of this DPA, including by implementing and maintaining appropriate technical and organizational measures to protect the Personal Data they Process consistent with Appendix 1. Netskope will maintain an up-to-date list of Sub-processors, which will be available at https://www.netskope.com/netskope-sub-processors and upon request via email to privacy@netskope.com. Netskope will update the list at least thirty (30) days prior to adding or changing Sub-processors and provide notice to Customer's designated support contacts. Where Customer has been provided notice of an intended change in Sub-processor, and Customer does not object within thirty (30) days after notice, Customer will be deemed to have consented to use of the Sub-processor. If Customer reasonably objects to a change in Sub-processor for security or compliance reasons, then the parties shall discuss possible alternatives. If Netskope does not provide a reasonably acceptable alternative to the objected-to Sub-processor, then Customer may terminate the affected Services and receive a prorated refund of fees paid for the remaining period of Services after termination.

5.2. Liability. Netskope shall be liable for the acts and omissions of its Sub-processors to the same extent Netskope would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1. Controls for the Protection of Personal Data. Netskope shall maintain appropriate administrative, physical and technical safeguards to maintain the security, confidentiality and integrity of Customer Data, including Personal Data, as set forth in the Security Specifications. Netskope regularly monitors compliance with these safeguards. Netskope will not materially decrease the overall security of the Services during the term of the Agreement.

6.2. Third-Party Certifications and Audits. Netskope has obtained third-party certifications and audits as set forth in the Security Specifications. Upon Customer's written request, at reasonable intervals, Netskope shall provide a copy of Netskope's then most recent third-party audit or certification, as applicable, or any summaries thereof, that Netskope generally makes available to its Customers at the time of such request.

7. SECURITY INCIDENT MANAGEMENT AND NOTIFICATION

7.1. Security Incident Notification. Netskope maintains security incident management policies and procedures as indicated in the Security Specifications and shall, without undue delay, notify Customer of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data of which Netskope becomes aware (a "Security Incident").

7.2. Security Incident Response. To the extent such Security Incident is caused by Netskope or systems under its control, Netskope shall: (i) reasonably cooperate with Customer to investigate and resolve the Security Incident; (ii) make reasonable efforts to identify and remediate the cause of such Security Incident; and (iii) keep Customer up-to-date about developments in connection with the Security Incident.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1. At Customer's election, following termination or expiration of the Agreement, Netskope shall either return or delete Customer Data in accordance with the Agreement and Netskope's retention cycle.

9. ADDITIONAL TERMS FOR EU PERSONAL DATA

9.1. Objective and Duration. The objective of Processing of Personal Data by Netskope is the performance of the Services pursuant to the Agreement.

9.2. Instructions. This DPA and the Agreement are Customer's complete instructions to Netskope in relation to the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately by the Parties.

9.3. Sub-processors. Customer acknowledges and expressly agrees that Netskope may retain and use Sub-processors in accordance with Section 5.1.

10. PRIVACY SHIELD

10.1. Self-certification. Netskope has self-certified under Privacy Shield so as to ensure that adequate safeguards are adduced with respect to the protection of privacy and fundamental rights and freedoms of individuals located in the EEA and Switzerland for the transfer of any Personal Data by Customer to Netskope. Accordingly, Netskope agrees to process any such Personal Data in compliance with the Privacy Shield Principles.

10.2. Sub-processing. Netskope agrees to remain responsible for any Personal Data received from Customer under Privacy Shield which is subsequently transferred to a Sub-processor.

10.3. Conflict. In the event of any conflict or inconsistency between this DPA and the Privacy Shield Principles, the Privacy Shield Principles shall prevail.

10.4. Adequacy. In the event that during the term of the Agreement Netskope is no longer self-certified under Privacy Shield, Netskope shall notify Customer and continue to process any Personal Data previously transferred under the Privacy Shield in accordance with the Privacy Shield Principles. In addition, Netskope shall do all such things as are legally required to ensure adequate protection for Personal Data in accordance with Data Protection Requirements. Such measures may include Netskope and Customer enter into Standard Contractual Clauses approved by the

European Commission or implementing an alternative data export adequacy measure permitted by Data Protection Requirements.

11. DATA TRANSFERS

11.1. Standard Contractual Clauses. Subject to Schedule 1, Customer (as "data exporter") and Netskope (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from Customer to Netskope.

11.1.1. The Standard Contractual Clauses shall come into effect under section 11.1 on the later of:

11.1.1.1. the data exporter becoming a party to them;

11.1.1.2. the data importer becoming a party to them; and

11.1.1.3. commencement of the relevant Restricted Transfer.

11.1.2. Section 11.1 shall not apply to a Restricted Transfer where a suitable alternative, which, for the avoidance of doubt, does not include obtaining consents from Data Subjects, is in place so as to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law. Such suitable alternative may include the EU-U.S. or Swiss-U.S. Privacy Shield, Binding Corporate Rules or other mechanism permitted under the GDPR.

11.1.3. Netskope warrants and represents that any Restricted Transfer to a Netskope Affiliate shall be made pursuant to the Standard Contractual Clauses unless section 11.1.2 applies.

12. AUDIT

12.1. Customer may, at its sole expense, perform a confidential “desk” or onsite audit (collectively “Customer Audit”) of Netskope’s compliance with this DPA specifically related to the Services under the Agreement. Any Customer Audit shall be conducted not more than once per year. Any onsite audit shall be conducted during Netskope’s regular business hours on a mutually agreed upon date, no earlier than thirty (30) calendar days after Netskope’s receipt of Customer’s written request for an audit. The audit shall be limited to security systems as they pertain to the Services and shall not exceed a cumulative eight (8) hours at Netskope’s facilities unless agreed in writing prior to any visit. If the audit exceeds the eight (8) hour period, Customer shall be responsible for payment of professional services fees to Netskope at the current hourly rate for professional services. Where Customer elects to have third party perform an audit on Customer’s behalf, such third party shall (i) not be a direct or indirect competitor of Netskope, and (ii) execute a confidentiality and non-disclosure agreement as approved by and for the benefit of Netskope. Upon completion of the audit, Customer shall promptly provide Netskope a summary of any findings from each report prepared in connection with the audit and the Parties shall discuss the results, including any suggested remediation. If the audit results find Netskope is not in substantial compliance with the requirements of this DPA, then Customer shall be entitled, at Netskope’s expense, to perform up to one (1) additional such audit in that year in accordance with the procedure set forth in this Section. Netskope agrees to work with Customer to identify reasonable remediation actions and to promptly take action at Netskope’s expense to address those matters or items upon which the Parties mutually agree require correction. The audit processes set forth in this Section are commercial in nature and shall not be deemed to restrict any audit rights provided in the Standard Contractual Clauses.

13. GOVERNING LAW

13.1. The Governing Law and Disputes provisions contained within the Agreement shall apply to and be incorporated by reference into this DPA unless and to the extent the Data Protection Requirements require otherwise, in which case this DPA will be governed in accordance with such Data Protection Requirements.

14. LEGAL EFFECT

14.1. This DPA shall only become legally binding between Customer and Netskope when executed in full.

Data Controller	**Data Processor - Netskope, Inc.**
SIGNATURE: ________________________________	SIGNATURE: DocuSigned by: James Bushnell F8CD777A6C164D3...
NAME: ________________________________	NAME: James Bushnell
TITLE: ________________________________	TITLE: Vice President, Legal Affairs
DATE: ________________________________	DATE: January 28, 2019

APPENDIX 1 TO THE DATA PROCESSING AGREEMENT

SECURITY SPECIFICATION REQUIREMENTS

Organizational Security Measures

Netskope implements various technical and organizational measures designed to ensure a level of security appropriate to the risks posed to Personal Data and Data Subjects. Such measures seek to prevent unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Personal Data Processing.

Consistent with the guidelines set forth in Article 32 of the GDPR and taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purposes of Processing, such measures include:

Access Control of Data Processing Areas

Netskope implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (infrastructure, databases and application servers and related hardware) where the Personal Data are Processed or used.

This is accomplished by:

- establishing security areas & realms;
- protection and restriction of access paths, logical and physical;
- securing the data processing equipment and personal computers;
- establishing access authorizations for employees and third parties, including the respective documentation;
- regulations and restrictions on use of access card-keys;
- all of the data centers where personal data are hosted:
- have all access logged, monitored, and tracked;
- are secured with locks, badge readers, biometric access controls, man-traps; and
- are secured by a security alarm system and other appropriate security measures including continuous CCTV.

Access Controls to Data Processing Systems

Netskope implements suitable measures to prevent its data processing systems from being used by unauthorized persons.

This is accomplished by:

- identification of the terminal and/or the terminal user to the Netskope systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- User IDs are monitored and access revoked when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes and secure tokens;
- strong password requirements (minimum length, use of special characters, re-use, etc.);
- protection against external access by means of a state-of-the-art industry standard firewall and/or appropriate network security controls whose connection to the intranet [if applicable] shall in addition be safeguarded by a VPN connection;
- dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions; and
- all access to data content on machines or computer systems is logged, monitored, and tracked.

Access Controls to Use Specific Areas of Data Processing Systems

Netskope commits that the persons entitled to use its data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization.

This is accomplished by:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the Personal Data;
- effective and measured disciplinary action against individuals who access Personal Data without authorization;
- release of data to only authorized persons;
- control of files, controlled and documented destruction of data; and
- policies controlling the retention of back-up copies.

Transmission Controls

Netskope implements suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.

This is accomplished by:

- use of managed industry standard firewalls and encryption technologies to protect the gateways and data pipelines through which the data travels;
- use of TLS (with strong cipher suites) encryption for all http-connections;
- implementation of secure two-factor VPN connections to safeguard the connection to the internet, if applicable;
- encryption of Personal Data by industry standard encryption technology (with strong cipher suites), if applicable;
- constant monitoring of infrastructure (i.e. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and
- monitoring of the completeness and correctness of the transfer of data (end-to-end integrity checks).

Input Controls

Netskope implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed.

This is accomplished by:

- an authorization policy for the input of data into hosted service, as well as for the reading, alteration and deletion of stored data;
- authentication of the authorized personnel;
- protective measures for the data input, as well as for the reading, alteration and deletion of stored data;
- utilization of user codes (passwords and tokens);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user ID's that have not been used for a substantial period of time;
- logging or otherwise evidencing input authorization and electronic recording of entries.

Instructional Controls

Netskope ensures that Personal Data may only be Processed in accordance with the Netskope Customer Agreement together with any reasonable and relevant instructions received in writing from authorised personnel of the Customer from time to time which may be specific instructions or instructions of a general nature as set out in the Netskope Customer Agreement or as otherwise agreed between the Customer and Netskope during the term of the Netskope Customer Agreement. This is accomplished by binding policies and procedures for Netskope's employees.

Availability Controls

Netskope implements suitable measures to ensure that Personal Data are protected from accidental destruction or loss.

This is accomplished by:

- Infrastructure redundancy: Netskope service data including any applicable personal data is stored on hardware with redundant disks and subsystems which are replicated in real-time and, where applicable, are also backed up daily across geographically segregated data centers.

Separation of Processing for different Purposes

Netskope implements suitable measures to ensure that data collected for different purposes can be processed separately.

This is accomplished by:

- access to data is separated through multiple diverse applications for the appropriate users; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is Processed separately.

APPENDIX 2 TO THE DATA PROCESSING AGREEMENT

Data Controller: Customer
Data Controller is: (i) the legal entity that has executed the Standard Contractual Clauses as a Data Controller; and (ii) any Customer Affiliates established within the European Economic Area (EEA) and Switzerland that have purchased the Services as set forth in the Agreement.

Data Processor: Netskope, Inc.
Data Processor is a provider of Cloud security services, which processes personal data upon the instruction of the Data Controller in accordance with the terms of the Service Agreement.

Data subjects
Data Controller has instructed Netskope to collect and host certain information in the course of its employee's use of Data Controller systems, to enable Data Controller to secure its systems from compromise. The information submitted may include Personal Data provided by the individual data subject or Data Controller in accordance with the relevant Services selected. The extent of the Personal Data collected is determined and controlled by the Data Controller in its sole discretion, and may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees or independent contract persons of Data Controller
- Data Controller's users authorized by Data Controller to use the relevant Service(s)

Categories of data
The personal data processed concern the following categories of data:

- name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number;
  - Source IP address of the user
  - Active Directory name of the user
  - Organizational unit (OU) mapping of the user in Active Directory (AD) (conditional, if exposed by the logs)
  - Cloud application accessed by the user [No personal data]
  - Activity performed by the user in the cloud application [activity limited to data exchange interfaces]
  - Active Directory name and/or email alias of parties that data is shared with through the cloud application

Special categories of data (if appropriate)
None

Processing operations
When performing the Services, the Data Processor (Netskope) will process the Personal Data on behalf of the Data Controller for the following Purpose(s): Delivering services subject to the Service Agreement, including but not limited to Cloud security services includes processing of web gateway / proxy logs and analyse logs to provide detailed reporting on application usage, data flow, user access to applications; This work may extend to other important applications logs of Data Controller for the purpose of log analysis and reporting on application usage, dataflow and user access.

SCHEDULE 1 – STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

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

Customer and/or its Affiliate(s)
(as described in the attached Data Processing Addendum)

…………………………………………………………
(the data **exporter**)

And

Netskope, Inc and/or its Affiliate(s)
(as described in the attached Data Processing Addendum)
2445 Augustine Dr., Suite 301, Santa Clara, CA 95054, United States of America

………………………………………………………………
(the data **importer**)

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;

(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 organisational security measures'* means those measures aimed at protecting 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.

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. 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): …

Position: …

Address: …

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

Signature:

On behalf of the data importer:

Name (written out in full): James Bushnell

Position: Vice President of Legal Affairs

Address: 2445 Augustine Dr., Suite 301, Santa Clara, CA 95054, United States of America

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

Signature: DocuSigned by:
James Bushnell
F8CD777A6C164D3...

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 "Customer"

Data importer
The data importer is Netskope
Data processor as defined in the Agreement (including the Addendum).

Data subjects
The personal data transferred concern the following categories of data subjects:
The categories of Data Subjects as defined and set forth in the Agreement (including the Addendum).

Categories of data
The personal data transferred concern the following categories of data (please specify):
The categories of Personal Data as defined and set forth in the Agreement (including the Addendum).

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
The special categories of Personal Data as defined and set forth in the Agreement (including the Addendum).

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
For the Permitted Purpose(s) as set forth in the Agreement (including the Addendum).

Data Exporter	**Data Importer**
Customer	*Netskope*
Attn:	*Attn: James Bushnell*
Address shall be the address of Customer as described in the attached Data Processing Addendum	Address shall be the address of Netskope, Inc. as described in the attached Data Processing Addendum
The Data Exporter's acceptance of the attached Data Processing Addendum shall constitute its agreement to these Standard Contractual Clauses	***The Data Importer's acceptance of the attached Data Processing Addendum shall constitute its agreement to these Standard Contractual Clauses***

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):

Data importer shall maintain the appropriate technical and organizational measures to protect Personal Data provided by data exporter (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), and to ensure the confidentiality and integrity of such Personal Data.

Data Exporter	**Data Importer**
Customer	*Netskope*
Attn:	*Attn: James Bushnell*
Address shall be the address of Customer as described in the attached Data Processing Addendum	Address shall be the address of Netskope, Inc. as described in the attached Data Processing Addendum
The Data Exporter's acceptance of the attached Data Processing Addendum shall constitute its agreement to these Standard Contractual Clauses	***The Data Importer's acceptance of the attached Data Processing Addendum shall constitute its agreement to these Standard Contractual Clauses***