ZSCALER PARTNER DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into between Zscaler, Inc., located at 120 Holger Way, San Jose, CA 95134, USA ("**Zscaler**" or "**Data Importer**"), and Partner ("**Partner**" or "**Data Exporter**").

HOW THIS DPA APPLIES

This DPA is only valid and legally binding if (i) the Partner entity agreeing to be bound by this DPA is a party to an Agreement and this DPA is required under applicable Data Protection Legislation (defined below); (ii) Zscaler processes Partner's Personal Data (defined below); or (iii) Partner processes a Zscaler Customer's (defined below) personal data in order to provide support services to a Zscaler Customer.

The parties hereby agree that the terms and conditions in this DPA, including all Exhibits, are expressly incorporated into the Agreement, and to the extent of conflict, the terms, and conditions in this DPA related to the processing Personal Data in connection with the Agreement will supersede the conflicting term or condition in the Agreement.

INSTRUCTIONS FOR MODIFYING THIS DPA

This DPA consists of this cover page, the DPA Terms, Exhibit A, Exhibit B, Exhibit C (with its Annex I and Annex II) and Exhibit D. Any modifications to the terms of this DPA (whether handwritten or otherwise) will render this DPA ineffective unless Zscaler has separately agreed to those modifications in writing. If you have any questions about this DPA, please contact privacy@zscaler.com

DPA TERMS

1. DEFINITIONS. Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1.1 "**Agreement**" means the Reseller Agreement or any other agreement between Zscaler and a specific Partner under which Partner is authorized to resell, provide managed services, and/or otherwise provide the Products to Customers.

1.2 "**Controller**", "**data subject**", "**personal data breach**," "**process**", "**processing**", "**processor**", and "**supervisory authority**" shall have the meanings given in applicable Data Protection Legislation or, if not defined in applicable Data Protection Legislation, the GDPR.

1.3 "**Customer**" means the end user customer who (i) orders the Products from Partner; and/or (ii) engages Partner as a managed service provider on behalf of Zscaler to use the Products for its internal purposes in the Territory.

1.4 "**Data Exporter**" means the controller who transfers the Personal Data to a Data Importer.

1.5 "**Data Importer**" means the processor who agrees to receive Personal Data from the Data Exporter intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the applicable Transfer Mechanism.

1.6 "**Data Protection Legislation**" means all laws and regulations applicable to the processing of Personal Data under the Agreement, as amended or replaced from time to time, including but not limited to laws and regulations of the European Union, the European Economic Area (EEA) and their member states, Switzerland, and the United Kingdom, such as 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 (the "**GDPR**").

1.7 "**Partner**" means the entity that is a party to the Agreement, including any Partner affiliates.

1.8 "**Customer Personal Data**" means any Customer information which is related to an identified or identifiable natural person that is submitted by Partner to Zscaler for the purposes of (i) reselling the Products to Customer; and/or (ii) providing managed services to Customer on behalf of Zscaler. The types of Personal Data and the specific uses of the Personal Data are detailed in **Exhibit A (Data Processing Details)** attached hereto.

1.9 "**Products**" means the Zscaler services and products ~~(i)~~ ordered by Partner for Customer(s) in an Agreement

2. DATA PROCESSING.

2.1 **Roles of the Parties**. The parties acknowledge and agree that with regard to this DPA, Zscaler is either the processor or sub-processor of Partner. Zscaler shall process Personal Data to provide the Products.. In order for Partner and Zscaler to administer the terms of the Agreement and this DPA personal information may be processed. For such processing Partner and Zscaler will act as an independent data Controller and process such data in compliance with applicable Data Protection Legislation.

2.2 **Processing Instructions**. Partner instructs Zscaler to process Customer Personal Data for the following purposes: (a) processing necessary for the provision of the Products and in accordance with the Agreement; and (b) processing to comply with the other reasonable written instructions provided by Partner to where such instructions are consistent with the terms of the Agreement, as required to comply with applicable Data Protection Legislation, or as otherwise mutually agreed by the parties in writing. Zscaler will promptly inform Partner if, in its opinion, compliance with any Customer instructions would infringe Data Protection Legislation.

2.3 **Zscaler Processing of Personal Data**. Zscaler will process Customer Personal Data as follows~~:~~

(a) Zscaler will process the Customer Personal Data only in accordance with any documented instructions with respect to the processing of such Customer Personal Data and in a manner necessary for the provision of the Products by Zscaler which will, for the avoidance of doubt, includes processing in accordance with the Agreement and this DPA;

(b) Zscaler will comply with applicable Data Protection Legislation;

(c) Zscaler will implement appropriate technical, administrative, physical and organizational measures to adequately safeguard and protect the security and confidentiality of Customer Personal Data against accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access;

(d) Zscaler will ensure that persons authorized to process Customer Personal Data on behalf of Zscaler have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(e) Zscaler will, taking into account the nature of the processing, assist with the fulfillment of data subject's rights requests for with respect to Personal Data using appropriate technical and organization measures. To the extent legally permitted, Partner shall be responsible for any reasonable costs that Zscaler may incur in providing such assistance;

(f) Zscaler will reasonably assist Partner in complying with its obligations with respect to Customer Personal Data pursuant to applicable Data Protection Legislation;

(g) Zscaler and its representatives will cooperate, upon request, with the relevant supervisory authority in regards to providing the Products;

(h) Zscaler will, upon request, and subject to the terms of the Agreement and this DPA (i) delete or return all Customer Personal Data after the end of the provision of the Products, and (ii) delete existing copies of Customer Personal Data unless legally required to retain the Customer Personal Data; and

(i) Zscaler will maintain a record of all categories of processing activities carried out to provide the Products. Zscaler will make available to Partner or relevant supervisory authority, if requested, all information necessary to demonstrate Zscaler's compliance with its obligations under applicable Data Protection Legislation.

3. RIGHTS OF DATA SUBJECTS.

Taking into account the nature of the processing, the party's shall assist each other in the fulfilment of a party's obligation to respond to a data subject request under applicable Data Protection Legislation. In addition, to the extent Partner, does not have the ability to address a data subject request, Zscaler shall upon Partner's request provide commercially reasonable efforts to assist Partner in responding to such data subject request. To the extent Zscaler is legally permitted to do so and the response to such data subject request is required under applicable Data Protection Legislation. To the extent legally permitted, Partner shall be responsible for any reasonable costs that Zscaler may incur in providing such assistance.

4. INTERNATIONAL TRANSFERS.

4.1 International Transfers. Zscaler may process or transfer Customer Personal Data in or to a territory other than the territory in which such data was first collected. For clarity, Zscaler shall take such measures as are necessary to ensure such processing or transfer is in compliance with applicable Data Protection Legislation.

4.2 Transfer Mechanism. If applicable Data Protection Legislation places restrictions on the transfer of Customer Personal Data across international borders, then Zscaler will ensure that any international transfer is performed in accordance with applicable Data Protection Legislation and, if required, the parties will execute such applicable legal mechanism ("**Transfer Mechanism**"). This includes executing the following Transfer Mechanisms as part of this DPA:

4.2.1.1 EU Standard Contractual Clauses. If Customer Personal Data is transferred outside of the EEA or Switzerland to a country that is not subject to or recognized by the GDPR to offer an adequate level of protection for Personal Data and is not covered by a suitable framework recognized by relevant authorities or courts that offer an adequate level of protection for Customer Personal Data, in the course of meeting the parties obligations hereunder Zscaler agrees to, and shall comply with, the EU Standard Contractual Clauses – Module Two: Controller to Processor and Module Three: Processor to Processor ("EU SCCs"), and all annexes attached thereto, as applicable. Where Module Two and Three have options, they will be selected and apply as such; Clause 7 will not apply, Clause 9 Option 2 will apply, the optional language in Clause 11 will not apply, Clause 17 Option 2 will apply and specify Ireland, and Clause 18 will specify Ireland. Such clauses shall be incorporated herein by this reference automatically and supersede prior Standard Contractual Clause versions as of the date they become effective as set by the EU Commission.

4.2.1.2 Switzerland's Federal Act on Data Protection. All references to the GDPR in the EU SCCs should be understood as references to the Federal Act on Data Protection ("FADP") of Switzerland insofar as the data transfers are subject to the FADP. Insofar as the data transfers are subject to the FADP, the EU SCCs will be governed by the law of Switzerland. The term "Member State" in the EU SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of claiming their rights in their habitual place of residence (Switzerland) in accordance with Clause 18(c) EU SCCs.

4.2.1.3 United Kingdom (UK) International Data Transfer Addendum to the European Commission's Standard Contractual Clauses. If Customer Personal Data is transferred outside of the United Kingdom to a country that is not recognized to offer an adequate level of protection for Customer Personal Data and is not covered by a suitable framework recognized by relevant authorities or courts that offer an adequate level of protection for Customer Personal Data, and subject to the UK GDPR in the course of meeting the parties obligations hereunder Zscaler agrees to and shall comply with, the UK International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for international data transfers ("UK Clauses"), as applicable. Should the appropriate UK regulatory authority issue and require use of updated contractual clauses, such clauses shall be incorporated herein by this reference automatically and supersede prior versions as of the date they take effect under UK law.

4.3 Alternative Transfer Mechanism. Zscaler agrees to notify Partner if it determines that a change in applicable Data Protection Legislation will adversely affect or invalidate the warranties and obligations provided under an executed Transfer Mechanism or if an alternative Transfer Mechanism becomes available to use by the parties. In such an event, Zscaler will work with

the Partner to find a mutually agreeable solution to ensure that Customer Personal is transferred in compliance with applicable Data Protection Legislation.

5. SUB-PROCESSORS.

5.1 Sub-processing. Partner provides a general authorization to Zscaler to engage sub-processors that are listed at the following link: https://www.zscaler.com/legal/subprocessors ("**Sub-processors**") to enable Zscaler to fulfill its contractual obligations under the Agreement and this DPA. For purposes of clarity, Sub-processors may include Zscaler affiliates.

5.2 Sub-processor Agreements. Zscaler will: (a) enter into a written agreement and) ensure that each such written agreement contains terms that are no less protective of Customer Personal Data than those contained in this DPA; and be liable for the acts and omissions of its Sub-processors to the same extent that Zscaler would be liable if it were performing the services of each of those Sub-processors directly under the terms of this DPA. Upon written request by Partner, copies of Sub-processor agreements may be provided to Partner in a manner to be determined by Zscaler. The parties agree that copies of any Sub-processor agreements that are provided by Zscaler to Partner may have all commercial information, business secrets, or other confidential information redacted by Zscaler beforehand.

5.3 Changes to Sub-processor List. Zscaler will provide Partner with advance notice before a new Sub-processor processes any Customer Personal Data. Partner may object to the new Sub-processor within fifteen (15) days of such notice on reasonable grounds relating to the protection of Customer Personal Data by following the instructions set forth in the Sub-processor List. In such case, Zscaler shall have the right to cure the objection through one of the following options: (1) Zscaler will cancel its plans to use the Sub-processor with regards to processing Customer Personal Data or will offer an alternative to provide the Products without such Sub-processor; or (2) Zscaler will take the corrective steps requested by Partner in its objection notice and proceed to use the Sub-processor; or (3) Zscaler may cease to provide or Partner may agree not to use whether temporarily or permanently the particular aspect or feature of the Product that would involve the use of such Sub-processor. If none of the above options are commercially feasible, in Zscaler's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days after Zscaler's receipt of Partner's objection notice, then either party may terminate the Agreement for cause without a refund of any pre-paid fees. Such termination right is Partner's sole and exclusive remedy if Partner objects to any new Sub-processor.

6. SECURITY MEASURES.

Zscaler will implement appropriate technical, administrative, physical and organizational measures set forth in **Exhibit B (Zscaler Data Protection and Information Security)** to adequately safeguard and protect the security and confidentiality of Customer Personal Data against accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access ("**Security Measures**"). Zscaler will not materially decrease the overall security of the Products during the term of the Agreement. Zscaler will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors, and Sub-processors to the extent applicable to their scope of performance.

7. SECURITY INCIDENT NOTIFICATION.

If ~~a party~~ Zscaler becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer Personal Data, then will notify Partner without undue delay after becoming aware of and confirming the Security Incident. Zscaler will take reasonable steps to: (a) identify the cause of the Security Incident; and (b) take any actions necessary and reasonable to remediate the cause of such Security Incident to the extent such remediation is within reasonable control. Zscaler will also reasonably cooperate with Partner with respect to any investigations and with preparing potentially required notices, and provide any information reasonably requested in relation to the Security Incident.

8. AUDITS

Zscaler acknowledges that Customers may exercise audit rights, as required under applicable Data Protection Legislation (the "**Audit"**), regarding processing and protection of Customer Personal Data under applicable Data Protection Legislation, and that a Partner may conduct an Audit on behalf of the Customer if such right has been assigned by Customer to Partner in writing. Such audit will be carried out in accordance with the following conditions:

(a) An Audit of its data processing facilities may be performed no more than once per year during Zscaler's normal business hours, unless otherwise agreed to in writing by Partner and Zscaler or required under applicable Data Protection Legislation;

(b) Zscaler will receive at least thirty (30) days' prior written notice of an Audit, which may be conducted by Partner or an independent auditor that is not a competitor of Zscaler ("**Auditor**");

(c) The Auditors will conduct Audits subject to any appropriate and reasonable confidentiality restrictions requested by Zscaler;

(d) The scope of an Audit will be limited to Zscaler systems, processes and documentation relevant to the processing and protection of Customer Personal Data;

(e) Prior to the start of an Audit, the parties will agree to reasonable scope, time, duration, place and conditions for the Audit, and a reasonable reimbursement rate payable by Partner to Zscaler for Zscaler's Audit expenses;

(f) If available, Zscaler will provide an Auditor, upon request, with any third party certifications pertinent to Zscaler's compliance with its obligations under this DPA (for example, ISO 27001 and/or SOC 2, Type II); and

~~**(g)**~~ Zscaler will receive prompt notice ~~and provide Zscaler~~ with full details regarding any perceived non-compliance or security concerns discovered during the course of an Audit~~; and~~

9. GENERAL.

9.1 Term and Termination. This DPA will remain in force until (i) it is replaced or repealed by mutual agreement of Partner and Zscaler, or (ii) the Agreement is terminated or expires.

9.2 Liability. Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Agreement. Each party's liability to the other party under this DPA will be limited to the same extent as its liability under the Agreement. For the avoidance of doubt, the total liability of a party and its affiliates for all claims by the other party or a third party arising out of or related to the Agreement and this DPA shall apply in aggregate for all claims under both the Agreement and this DPA. In no event will either party limit its liability with respect to any data subject rights under any relevant clauses in an applicable Transfer Mechanism.

9.3 Governing Law. Without prejudice to any relevant clauses relating to the governing law in an applicable Transfer Mechanism cited in Section 4.2 (Transfer Mechanism) of this DPA: (i) the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and (ii) this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

9.4 Changes in Data Protection Legislation. Zscaler and Partner may, by written notice to the other party, propose to amend the appendices to any applicable Transfer Mechanism or this DPA as required as a result of any change in, or decision of a competent authority under, applicable Data Protection Legislation, to allow processing of Personal Data to be done (or continue to be done) without breach of such Data Protection Legislation. The parties agree to make any such required amendment, which shall be in writing and signed by both parties.

9.5 Counterparts. This DPA may be executed in any number of counterparts, each of which will be deemed to be an original and all of which taken together will comprise a single instrument. This DPA may be delivered by facsimile or electronic document format (e.g. PDF), and facsimile or electronic copies of executed signature pages will be binding as originals.

9.6 Entire Agreement. This DPA, together with the Agreement, constitutes the entire agreement between the parties and supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. In case of conflict or inconsistency between this DPA, the Agreement, and the applicable Transfer Mechanism cited in Section 4.2 (Transfer Mechanism) of this DPA, the following order of precedence shall govern to the extent of the conflict or inconsistency: (i) the applicable Transfer Mechanism; (ii) this DPA; and (iii) the Agreement.

9.7 Severability. If any provision of this DPA is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed, and the remainder of terms will remain in full effect.

Exhibit A

Data Processing Details

Subject Matter of Processing	The subject matter of Processing is the Products pursuant to the Agreement.
Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
Categories of Data Subjects	The employees, contractors, or other third party users of Partner's Customers.
Nature and Purpose of Processing	Nature: Processing as part of the Products ordered by Customer in the Agreement. Purpose: The purpose of the Processing of Customer Personal Data by is to provide the Products to a Customer pursuant to the Agreement.
Types of Personal Data	Includes the following: - Names - Email addresses - Addresses - Customer Personal Data - Other data provided ~~by Partner~~ to facilitate the Zscaler's provision of Products to Customer under the Agreement.

Exhibit B

Zscaler Data Protection and Information Security

This **Exhibit B** shall be incorporated by reference into the Zscaler Data Processing Agreement ("**DPA**") executed between the parties. Capitalized terms not defined herein shall have the meanings assigned to such terms in the DPA or Agreement.

1. Secure Files. Throughout the Customer's Subscription Term of Zscaler's Products, Customer Personal Data in Zscaler's possession or control shall be subject to safeguarding and disaster recovery protection and shall be stored at secure physical or electronic facilities operated under Zscaler's control.

2. Data Availability. Zscaler shall adhere to appropriate technical and organizational measures that represent the best industry practices in the storage, safeguarding, and preservation of any Customer Personal Data in Zscaler's possession or control, including performing real-time backups to regional geographically disperse locations and ensuring the security (i.e., both physical and unauthorized remote access) of all hardware and equipment used to host or store such Customer Personal Data pursuant to the provisioning of the SaaS.

3. Safeguards and Controls. Zscaler agrees that during the Customer's Subscription Term of Zscaler's Products, and continuing as long as Zscaler controls, possesses, stores, transmits or processes Customer Personal Data, Zscaler and its subcontractors/sub-processors shall employ and maintain reasonable security measures to ensure that Customer Personal Data in Zscaler's possession or control is protected from unauthorized use, alteration, access or disclosure, and to protect and ensure the confidentiality, integrity and availability of such data, consistent with all applicable Data Protection Legislation. Such security measures shall include, but not be limited to, the following:

a) implementing reasonable restrictions regarding physical and electronic access to Customer Personal Data, including, but not limited to, physical access controls, secure user authentication protocols, secure access control methods, firewall protection, malware protection, anonymization, tokenization and use of encryption where appropriate or required by Data Protection Legislation;

b) maintaining a reasonable and appropriate written data security policy that includes technological, physical, administrative and procedural controls to protect the confidentiality, integrity and availability of Customer Personal Data, that encompasses access, retention, transport, and destruction of such Personal Data, and that provides for disciplinary action in the event of its violation;

c) preventing terminated employees from accessing Customer Personal Data by terminating without undue delay their physical and electronic access to Zscaler's Products;

d) employing assessment, monitoring and auditing procedures to ensure internal compliance with these safeguards;

e) conducting an independent security assessment of these safeguards at least annually, and, upon Partner's reasonable written request not more than once annually, providing certification to demonstrate compliance with all such applicable security requirements; and

f) only using Customer Personal Data for the purpose of providing the Products in accordance with the Agreement and DPA, and Zscaler shall not provide any other third party with access to Customer Personal Data, unless it has received prior written consent from Partner, or such access is specifically allowed under the Agreement and DPA.

4. Reporting. Zscaler shall maintain records, logs and reports concerning its compliance with Data Protection Legislation and/or relevant industry standards, security breaches, storage, processing, and transmission of Customer Personal Data in its possession or control.

As a condition of providing the Products, no less than once each calendar year, Zscaler will undergo, at its sole cost and expense, a Statement on Standards for Attestation Engagements (SSAE) No. 18 for Reporting on Controls at a Service Organization, Service Organization Controls (SOC) 2 Type 2 audit (or industry equivalent as the standard may progress). Upon Partner's written request, Zscaler will provide Partner with a copy of its most recent SSAE No. 18 SOC 2 Type 2 report on an annual basis, resulting from such audit and such other evidence, information and documentation as is reasonably necessary to demonstrate compliance with this Exhibit.

5. Security Incident Response. Zscaler shall maintain policies and procedures for responding to Security Incidents. In the event of a Security Incident involving unauthorized disclosure, loss, or destruction of Customer Personal Data in Zscaler's possession or control, Zscaler shall:

a) promptly and without undue delay investigate the reasons for and circumstances surrounding such Security Incident;

b) use best efforts and take all necessary actions to contain and mitigate the impact of such Security Incident;

c) provide written notice to Partner without undue delay after Zscaler confirms a Security Incident;

d) within five (5) days of confirming a Security Incident, Zscaler must provide a written report to Partner concerning such Security Incident detailing Zscaler's findings, and update such report periodically thereafter;

e) collect and preserve all evidence concerning the cause, remedial actions and impact related to such Security Incident, which shall meet reasonable expectations of forensic admissibility;

f) document the incident response and remedial actions taken in detail; and

g) so long as Zscaler is not required to violate the confidentiality obligations with any of its other customers, partners, or vendors, provide Partner with any relevant documents related to such Security Incident, including without limitation, any security assessment and security control audit reports, relevant logs and/or any forensic analysis of such Security Incident.

6. Destruction. Zscaler shall take all reasonable steps to ensure proper destruction (such that Customer Personal Data is rendered unusable and unreadable) after the expiration or earlier termination of the Agreement.

7. Management Direction for Information Security. Zscaler will assign a qualified member of its workforce with expertise in information security to be responsible for the development, implementation, and maintenance of Zscaler's enterprise information security program.

8. Organization of Information Security

a) Zscaler will ensure that the responsibilities of their workforce are appropriately segregated to reduce opportunities for unauthorized or unintentional access, modification, or misuse of the organization's assets.

b) Zscaler will maintain contact with the governing regulatory authorities to ensure ongoing compliance with the mandated regulatory requirements.

c) Zscaler will maintain appropriate contact with special interest groups, specialist security forums, and/or professional associations to remain abreast of evolving information security threats and trends.

d) As applicable, Zscaler will ensure that Information security is addressed within its internal project management processes.

9. Human Resources Security

a) Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

b) Zscaler will train new and existing employees and subcontractors to comply with relevant data security and data privacy obligations. Ongoing training is to be provided at least annually and more frequently as appropriate.

c) To the extent applicable, Zscaler will ensure that employees, contractors, sub-contractors or vendors are required to sign an agreement that contains confidentiality requirements at least as protective as those in the Agreement.

10. Asset Management

a) Zscaler will maintain an inventory of assets associated with information and information processing facilities.

b) Assets maintained in the inventory are assigned to an individual or group that is accountable and responsible for the assigned asset(s).

c) Acceptable use of assets is defined within a formal policy or standard.

d) The return of assets is clearly communicated, via policies and/or training, to all employees and external party users upon termination of their employment, contract or agreement. Return of assets is documented and tracked.

e) Zscaler classifies data in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. Procedures for handling assets are developed and implemented in accordance with this information.

11. Media Handling. Procedures are implemented for the management of removable media in accordance with the information classification.

12. Access Control

a) Zscaler will ensure that Partner's Confidential Information and Customer Personal Data will be accessible only by authorized personnel with appropriate user identification, two-factor authentication and access controls commensurate with information classification.

b) Two-factor authentication is required for remote connectivity.

c) Each authorized personnel shall have unique access credentials and shall receive training which includes a prohibition on sharing access credentials with any other person.

d) Zscaler will have a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services.

e) The allocation and use of privileged access rights will be restricted and controlled.

f) The allocation of secret authentication information is controlled through a formal management process.

g) User access rights are reviewed at regular intervals but at a minimum on an annual basis.

h) The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted as appropriate upon change in role or responsibilities.

i) Password management systems are interactive and ensure strong passwords.

13. Cryptography

a) Zscaler has a formal policy on the use of cryptographic controls for protection, including the use, protection and lifecycle of cryptographic keys.

b) Zscaler agrees that all Customer Personal Data will be protected and, where encrypted, will use a Federal Information Processing Standard (FIPS) compliant encryption product, also referred to as 140-2 compliant. Symmetric keys will be encrypted with a minimum of 128-bit key and asymmetric encryption requires a minimum of 1024 bit key length. Encryption will be utilized in the following instances:

   i. Customer Personal Data that is stored on any portable computing device or any portable storage medium.

   ii. Customer Personal Data that is transmitted or exchanged over a public network.

14. Physical and Environmental Security

a) A clear desk policy for papers and a clear screen policy for facilities processing Customer Personal Data is adopted and adhered to.

b) Systems are located in co-location facilities and are maintained by Zscaler personnel.

c) Only individuals on the approved access list can access Zscaler equipment and systems.

d) All facilities require badge and/or biometric access and have 24x7 security guards and CCTV.

e) Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

f) Access is created and maintained by Zscaler and only authorized to Zscaler personnel with a business need.

g) Visitors to the facility are required to be escorted at all times and are not allowed in caged areas.

15. Operations Security

a) Changes to the organization, business processes, information processing facilities and systems that affect information security shall be formally controlled.

b) Zscaler agrees that development and testing environments shall be separated from operational or production environments to reduce the risks of unauthorized access or changes to the operational or production environment.

c) Zscaler's software development processes and environment must protect against malicious code being introduced into its Product(s), future releases thereof, and/or updates thereto.

d) Zscaler shall have a dedicated team responsible for performing security audits, vulnerability scans, evaluating results and monitoring the remediation of technical vulnerabilities to ensure measures are taken to address the associated risk.

e) Zscaler software that controls access to Confidential Information or Customer Personal Data must log and track all access to the information.

   i. Logging facilities and log information shall be protected against tampering and unauthorized access.

   ii. Zscaler shall maintain access logs relevant to Customer Personal Data for the time period stated in the Agreement depending on the Product being used.

f) Rules governing the installation of software by Zscaler personnel are established and implemented on operational systems.

16. Network Security. Zscaler agrees to implement and maintain network security controls that conform to industry standards, including but not limited to the following:

a) Zscaler will appropriately segment its network to only allow authorized hosts and users to traverse areas of the network and access resources that are required for their job responsibilities.

b) Zscaler will ensure that publicly accessible servers are placed on a separate, isolated network segment typically referred to as the Demilitarized Zone (DMZ).

c) Zscaler will ensure that its wireless network(s) only utilize strong encryption, such as WPA2.

d) Zscaler will have an IDS and/or IPS in place to detect inappropriate, incorrect or anomalous activity and determine whether Zscaler's computer network and/or server(s) have experienced an unauthorized intrusion.

e) As appropriate, groups of information services, users and information systems shall be segregated on networks.

17. Data Transfers. Zscaler may transfer Customer Personal Data to provide our Products. The transfers of data may involve movement between jurisdictions and crossing international borders. Zscaler will ensure Customer Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transport or storage and that the transmission facilities receiving any Customer Personal Data can be established and verified. Practices implemented and maintained by Zscaler include, but are not limited to, the following:

a) All management connections to the servers occur over encrypted Secure Shell (SSH), Transport Layer Security (TLS) or Virtual Private Network (VPN) channels and remote access always requires multi-factor authentication.

b) Unless the connection originates from a list of trusted IP addresses, Zscaler does not allow management access from the Internet.

c) Zscaler maintains a change management system to submit, authorize, and review any changes made in the production environment.

d) Zscaler maintains a dedicated Network Operations Center (NOC), which is staffed 24/7.

18. Communications Security

a) Formal data transfer policies, procedures and controls shall be in place to protect the transfer of sensitive Confidential Information or Customer Personal Data within electronic messaging.

b) Zscaler will execute a data protection and information security agreement with electronic communication service providers to ensure that security controls meeting Zscaler's requirements have been implemented.

19. System Acquisition, Development, and Maintenance

a) Applicable information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

b) Confidential Information or Customer Personal Data involved in application services passing over public networks shall be protected from fraudulent activity, unauthorized disclosure, and modification.

c) Zscaler shall have policies that govern the development of software and systems and how information security and integrity are established and applied during development. Zscaler shall have a policy that outlines a governing framework to validate that security

controls are present in the solution to ensure confidentially, integrity and availability. Additionally, the policy will outline the processes, procedures, and standards to ensure no known security flaws have been introduced intentionally or unintentionally at any point in the Product's lifecycle or such time as the Product has formally reached end of life.

d) Upon initial hire or engagement of software developers, Zscaler shall provide them with secure software development training. Thereafter, Zscaler shall provide supplemental training periodically as necessary to address changing industry conditions and vulnerabilities. Any such training shall occur at least every two years.

e) Principles for engineering secure systems are established, documented, maintained, and applied to any information system implementation efforts.

f) Zscaler does not currently outsource system development responsibilities; however, should this change in the future, Zscaler shall supervise and monitor the activity of any such outsourced system development.

20. Service Provider Due Diligence

a) Zscaler will conduct due diligence reviews on our service providers who may have impact on Zscaler's ability to meet the requirements of the Agreement and this Exhibit.

b) Due diligence of such service providers shall include, but is not limited to, determining the appropriate information security requirements that should be included in agreements between Zscaler and its service providers.

21. Application and Software Security. Zscaler agrees that its Product(s) will, at a minimum, incorporate the following:

a) Zscaler uses third party auditors at least annually, to conduct automated (i.e., SAST, DAST and SCA) and manual security (i.e., penetration testing) assessments to ensure the Product codebase contains no known exploitable conditions classified as 'Critical/Very High' or 'High', or otherwise captured on the OWASP Top 10 or SAN Top 25 lists.

b) Zscaler agrees to provide, maintain and support its software and subsequent updates, upgrades, and bug fixes, such that the software is, and remains secure from Common Software Vulnerabilities in accordance with its product end of life (EOL) and end of sale (EOS) policy.

c) Zscaler agrees to provide updates and patches to remediate security vulnerabilities based on severity by CVSSv3 score and will work to remediate any known zero-day exploits without undue delay. In case of critical vulnerabilities, Zscaler will deploy mitigation with urgency upon discovering the issue and push out a patch without undue delay thereafter depending on risk level post mitigation.

22. Security Contact. The contact identified below shall serve as Zscaler's designated security contact for Partner security issues under this Agreement.

Zscaler Security Contact:

Name: Zscaler CISO Team

Address: 120 Holger Way

San Jose, CA 95134 USA

Email: ciso@zscaler.com