Cloud Service Provider Disclosure (SS 584:2020 MTCS)

The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, indicate accordingly in the remarks.

Date of disclosure: <u>11th November 2024</u>

Applicable cloud service(s): Zscaler Zero Trust Exchange

Cloud Service Provider Contact Information

Company name: Zscaler, Inc.

Primary address:

120 Holger Way

San Jose, California 95134

United States of America

Web address: https://www.zscaler.com

Contact name: Joshua Leong

Contact number: +81 80-7115-5341

Contact email: jleong@zscaler.com

Information security liaison:

Zscaler Compliance

120 Holger Way,

San Jose, California 95134

United States of America

Email: compliance@zscaler.com

Related affiliate for MTCS services:

ZSC Holdings Limited Singapore (UEN Registration no. T13FC0129E)

Singapore Land Tower, Levels 45-47, 50 Raffles Place

048623, Singapore

MTCS certificate number: <u>MTCS-2023-0017</u>

Company stamp: _____ Company representative signature: _____

Signed by:

Chris Potts

841B73E12C114B8...

Certification Body Contact Information

Company name: TÜV SÜD PSB Pte Ltd
Web address: https://www.tuvsud.com/sg

Contact name: Erichsen Soong

Contact number: 8777 5844   Contact email: erichsen.soong@tuvsud.com

Company stamp: Lead auditor signature:

Cloud Service Provider Background

Overview of service offering:

Zscaler leverages its Zero Trust Exchange platform with over 150 globally distributed locations to provide services that secure our customers' digital transformation activities such as Secure Services Edge(SSE) through Zscaler Internet Access(ZIA), universal Zero Trust Network Access(ZTNA) via Zscaler Private Access(ZPA), end to end visibility into worldwide user experience and network performance with Zscaler Digital Experience(ZDX) and workload security with Zscaler Posture Control(ZPC).

Service model:

☐ Virtual machine instances owned by the cloud service customer
☐ Network facilities
☐ Compliance with applicable standards

Deployment model:

☐ Private cloud
☐ Community cloud
☐ Hybrid cloud
☑ Public cloud

Tier:

☐ Level 1

☐ Level 2

☑ Level 3

No.	Criteria	Description	Remarks
		Legal and Compliance	
1.	Right to audit	The cloud service customer has the right to audit: ☐ Virtual machine instances owned by the cloud service customer ☐ Network facilities ☑ Compliance with applicable standards ☐ Technical controls ☐ Policies and governance ☐ Data centre facilities ☐ Others ☐ None Regulators recognised by Singapore law have the right to audit: ☐ Virtual machine instances owned by the cloud service customer ☐ Network facilities ☑ Compliance with applicable standards ☑ Technical controls ☑ Policies and governance ☑ Data centre facilities ☐ Others ☐ None Audit / assessment reports that can be made available on request: ☑ Penetration test ☑ Threat and vulnerability risk assessment ☑ Vulnerability scan ☑ Audit reports (e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation)	Zscaler possesses numerous security certifications under widely recognized schemes such as SOC2, multiple ISO standards, CSA STAR Level 2 etc., and makes related certificates and reports available to CSCs via its website so that they may verify compliance. Artifacts such as internal documents, details of configurations and access to physical sites may be provided only to authorized auditors if they are required to demonstrate compliance. As Zscaler provides its services under a SaaS model, the CSC does not own or operate any virtual machine instances.

2.	Compliance	The following guidelines / standards / regulations are adhered to: ☑ Singapore Personal Data Protection Act ☑ ISO/IEC 27001 ☐ ISO 9000 ☐ ISO/IEC 20000 ☑ CSA Open Certification Framework(CSA STAR) ☐ PCI-DSS ☑ Others: ISO 27701, ISO 27017, ISO 27018, SOC 2	Details of Zscaler's compliance with various standards and frameworks, including access to certificates and reports, may be found at https://www.zscaler.com/platform/privacy-and-compliance Zscaler has assessed its obligations under the Singaporean PDPA as a data intermediary and provides appropriate information customers about how these requirements are satisfied at https://www.zscaler.com/privacy-compliance/pdpa Zscaler is not within scope of the PCI DSS as it does not acquire, store or transmit any cardholder data, nor is it a TPSP vendor under the standard.
Data Control			
3.	Data ownership	All data on the cloud service is owned by the cloud service customer except for: _____ The cloud service customer retains the ownership on the derived data or attributes of cloud usage except for the following: ☐ Advertising or marketing ☐ Statistics analysis on usage ☐ Others _____	Customer data in the Zscaler cloud is limited to logs, which the customer retains ownership of.

| 4. | Data retention | Data deleted by the cloud service customer is retained as follows:

☐ Minimum data retention period is: _____
☐ Maximum data retention period is: _____
☐ Deleted immediately

Log data is retained for a period of:
☐ Minimum data retention period is: _____
☑ Maximum data retention period is: six months if storing logs in the Zscaler cloud
☐ Deleted immediately

Cloud service customer data is retained for a period of:

☐ Minimum data retention period is: _____
☐ Maximum data retention period is: _____
☑ Not retained

The following types of data are available for download by the cloud service customer:

☐ Log data
☐ Others _____ | Customer logs stored in the Zscaler cloud cannot be deleted for accountability purposes, and are retained for a rolling period of six months for most services.

Some Zscaler services have the option of a log streaming function which allows logs to be stored in customer-controlled storage like a SIEM, so that logs can be stored for any desired period. |
| 5. | Data sovereignty | The primary data locations are:

☐ Singapore
☐ Asia Pacific _____
☑ Europe(Germany, Netherlands, Switzerland)
☑ United States
☐ Others _____

The backup data locations are:

☐ Singapore
☐ Asia Pacific _____
☐ Europe _____
☐ United States
☐ Others _____

No. of countries in which data centres are operated: _____

The cloud service customer's data stored in the cloud environment will never leave the locations specified in item 5:

☑ Yes
☐ Yes, except as required by law
☐ Yes, except as noted: _____ | Sires storing customer data are limited to a small subset of locations as per item 5. The majority of Zscaler sites worldwide are points of presence that only serve to process customer traffic and do not save any data to disk.

Sites storing customer data synchronize with each other such that redundant copies of customer data exist in a geographically distributed fashion. Thus in the event of site failure, the service provision can failover seamlessly to the |

		Cloud service customer's consent is required prior to transferring data to a location not specified in item 5 or a third party: ☐ Yes ☐ Yes, except as required by law ☐ Yes, except as noted: _____ ☐ No *Note: Cloud service customers are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. In addition, cloud service customers should understand the risks associated with relevant laws that may allow for law enforcement or other government access to data in-transit or storage with Cloud Service Providers.*	other sites, mitigating the need for discrete backups.
6.	Non-disclosure	☑ Non-disclosure agreement template can be provided by Cloud Service Provider ☐ Cloud Service Provider may use customer's NDA (pending legal review)	Standard terms regarding confidentiality and treatment of confidential information are included in Zscaler's End User Subscription Agreement
Provider Performance			
7.	Availability	The committed network uptime is: ☐ _____% ☑ Varies according to price plan The committed system uptime is: ☐ _____% ☑ Varies according to price plan The cloud environment has the following single points of failure: ☐ _____ ☑ None	The availability of Zscaler services is dependent on the individual service, with key services such as ZIA and ZPA committing monthly uptimes of 100%, and other services committing minimum uptimes of 99.9%. All services are protected by SLA, the details of which can be viewed at https://www.zscaler.com/legal/sla-support

| 8. | 3rd party dependency | Highlight areas of critical dependency for service delivery:

Zscaler uses other cloud service providers such as Amazon AWS, Google Cloud Platform and Microsoft Azure to provide certain elements of the Zero Trust Exchange infrastructure. A full list may be found under the "Hosting Provider" heading of Zscaler's sub-processor listing here: https://www.zscaler.com/privacy-compliance/subprocessors

Where Zscaler owns and operates physical hardware infrastructure, it is located in colocation data centers operated by third party providers.

Risks and dependencies arising from the abovementioned providers are managed through Zscaler's third party risk management program, which requires thorough and cross-functional assessment and vetting of all vendors prior to onboarding and ongoing monitoring and review of risk assessments thereafter. | |
| 9. | BCP / DR | ☑ Disaster recovery protection
☑ Backup and restore service
☐ Cloud service customer selectable backup plans
☐ Escrow arrangements
☐ No BCP/DR is available
☐ RPO
☐ RTO
☐ Others, please specify:_____ | Zscaler maintains BCP and DRP procedures for its services to uphold the availability commitments in item 7. The geographically distributed architecture of the Zero Trust exchange means that it is resilient to localized disruptions.

Core services such as ZIA and ZPA have customer DR options such that they may still use the service in the event of an outage.

For some services, customers may |

			create a restore point of their configurations which they can roll back to at their choosing.
10.	Liability	The following terms are available for the cloud service customers on failure of the provider to meet the service commitment: ☐ Network failure Liability: _____ ☐ Infrastructure failure Liability: _____ ☐ Virtual machine instance failure Liability: _____ ☐ Migrations Liability: _____ ☑ Unscheduled downtime Liability: https://www.zscaler.com/legal/sla-support ☐ Database failure Liability: _____ ☐ Monitoring failure Liability: _____	Zscaler provides its customers with Service Level Agreements(SLAs) for each service as described in item 7.
11.	Shared responsibility	☑ Communication of shared roles & responsibilities for which CSC needs to implement and manage for use of this cloud service URL (or attach file): https://www.zscaler.com/legal/end-user-subscription-agreement	
Service Support			
12.	Change management	The Cloud Service Provider has established the following for changes, migrations, downtime, and other potential interruptions to cloud services: ☑ Communication plan and procedures for proactive notification ☐ Assistance in migration to new services when legacy solutions are discontinued ☐ Ability to remain on old versions for a defined time period ☐ Ability to choose timing of impact	Notifications of upgrades, maintenance and/or other changes is done proactively and as much as possible with prior notice via Zscaler's trust site(https://trust.zscaler.com)

13.	Self-service provisioning and management	Provide self-service provisioning and management portal for cloud service customers to manage cloud services: ☑ Yes ☐ No If yes, describe the functions of the self-service provisioning and management portal provided: ☑ Allow role-based access control (RBAC) ☑ Manage resource pools (e.g. VMs, storage, and network) and service templates ☐ Track and manage the lifecycle of each service ☑ Track consumption of services ☑ Health monitoring ☐ Others: _____	
14.	Incident and problem management	Delivery mode of support: ☑ Access via email ☑ Access via portal ☑ Access via phone support ☑ Direct access to support engineers Availability of support: ☑ 24 x 7 ☐ During office hours support, please specify the hours of operations: _____ ☐ After office hours support, please specify the hours of operations: _____ Service response time: As short as 15 minutes, depending on service tier Notification time of cloud service outage incident: Real time in so far as possible Communication channel used for notification of cloud service outage incident: Zscaler trust site(https://trust.zscaler.com) The following are available to cloud service customers upon request: ☐ Permanent access to audit records of customer instances ☐ Incident management assistance Incident response time: _____ Mean time to repair on detection of faults: _____	The details of support availability are dependent on the service and support tier package purchased by the customer, details of which are available at https://help.zscaler.com/phone-support

15.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☑ Pay per usage: Licenses for Zscaler services are charged by user count ☐ Fixed pricing _____ (up to yearly/monthly/daily) ☐ Other pricing model _____ ☐ Not disclosed Available billing history: _____ months	
16.	Data portability	Importable VM formats: _____ Downloadable formats: Some configuration data or templates can be downloaded as CSV, XML or similar format, but is unique to Zscaler and is not portable to other platforms. Supported operating systems: _____ Language versions of supported operating systems: _____ Supported database formats: _____ Policy/guide available: _____ API: ☐ Common_____ ☑ Customised: the customer can interact with Zscaler services using an API, details of which are available at https://help.zscaler.com Upon service termination or prolonged outage, data is available through: ☐ Physical media ☐ Standard methods as described above ☐ Other methods: _____	
17.	Interoperability	Use of industry standards and availability of APIs to support interoperability: ☑ Transport supported: REST-based HTTPS ☑ Format supported: Common formats such as CSV, XML, JSON etc. as applicable ☑ APIs supported differ by service, please see the guide for more information	

		☐ Other methods _____ Guide available on a per-service basis at https://help.zscaler.com	
18.	Access	Type of access to the service is through: ☑ Public access ☑ Private access (e.g. VPN, dedicated link) ☐ IPv6 access is supported ☐ Other access methods _____ Public access speed (shared bandwidth) in Mbps: _____	
19.	User Management	☐ Identity management ☐ Role based access control ☐ Federated access model ☑ Integration with Identity management solutions ☐ Others _____	Zscaler services operate through integration with the customer Identity Provider(IdP) using standard methods such as SAML federation. Zscaler does not provide identity management solutions.
20.	Lifecyle	The cloud service customer may select the following for service upgrades and changes: ☐ Automatic provisioning ☑ Cloud service customer customisable provisioning	
Security Configurations			
21.	Security configuration enforcement checks	Security configuration enforcement checks are performed: ☐ Manually ☑ Using automated tools How often are enforcement checks being performed to ensure all security configurations are applied? Weekly	Zscaler production environments are scanned by automated tools such as vulnerability scanners on a weekly basis
22.	Multi-tenancy	☐ Distinct physical hosts ☐ Distinct physical network infrastructure	Zscaler uses a multi-tenant

				architecture in which customer tenants and data are logically separated. The customer can configure security settings such as regarding access roles and authentication for their tenant through the Zscaler admin portal.
		☑ Virtual instance grouping ☑ Cloud service customer definable security domains ☑ Cloud service customer customisable firewall ☑ Cloud service customer definable access policies		
23.	Hybrid cloud provision	Ability to monitor, track, apply and enforce CSC's security & privacy policies on its cloud workloads: ☐ Data protection and encryption key mgmt. enforcement geolocation-based/resource pools and secure migration of cloud workloads ☐ Key mgmt. and keystore controlled by CSC ☐ Persistent data flow segmentation before and after geolocation based/resource pools secure migration ☐ Compliance enforcement for regulated workloads between on-premises private and hybrid/public cloud ☑ Others: Under some services such as ZIA and ZPA, Zscaler offers the ability for the customer to deploy appliances within the organization's network boundary that act as policy enforcement nodes. Thus, the customer retains some control over the security controls applied to the appliance and the environment in which it is operated.		
Service Elasticity				
24.	Capacity elasticity	The following capacity elasticity options are available: ☐ Programmatic interface to scale up or down ☐ Mean time to start and end new virtual instances _____ ☐ Alerts to be sent for unusual high usage ☐ Minimum performance during peak periods_____ ☐ Minimum duration to scale up computing resources _____ ☐ Minimum additional capacity guaranteed per account_____		The capacity of the Zero Trust Exchange infrastructure is managed by Zscaler and adjusted based on periodic review to ensure that it is able to meet customer demand.

25.	Network resiliency and elasticity	The following network resiliency and elasticity options are available: ☐ Redundant Internet connectivity links ☐ Redundant Internal connectivity ☐ Selectable bandwidth up to _____ Mbps ☐ Maximum usable IPs _____ ☐ Load balancing ports _____ ☐ Load balancing protocols _____ ☐ Anti-DDOS protection systems or services ☑ Defence-in-depth mechanisms, please specify: SSE security policy enforcement such as content and web app filtering, malware scanning and sandboxing, Zero Trust Network Access(ZTNA) to private apps etc. ☑ Network traffic isolation, please specify: Traffic bound for the Zero Trust Exchange can be routed through encrypted tunnels, high risk web access can be routed through browser isolation to prevent download and/or execution of malicious code ☐ Shared or dedicated bandwidth, please specify: _____ _____ ☑ QoS traffic control services ☑ Alerts to be sent for unusual high usage ☐ Minimum performance during peak periods _____ ☐ Minimum period to scale up network throughput _____	The options in item 25. are available as functions of Zscaler services such as ZIA and ZPA.
26.	Storage elasticity	The following storage redundancy and elasticity options are available: ☐ Redundant storage connectivity links within each data centre ☐ Redundant storage connectivity links between data centres belonging to the same cloud ☐ Storage traffic isolation, please specify: _____ ☐ Shared or dedicated storage network bandwidth, please specify: _____ ☐ Quality of service storage traffic control services ☐ Maximum storage capacity for entire cloud, please specify:_____ ☐ Maximum storage capacity for single cloud service customer, please specify: _____ ☐ Maximum expandable storage, please specify: _____ ☐ Alerts to be sent for unusual high usage ☐ Minimum storage I / O performance during peak periods _____	The Zero Trust Exchange does not offer data storage functions other than for customer logs.

		☐ Minimum period to scale up storage I / O throughput _____	