Cloud Service Provider Contact Information

Company name: Google Asia Pacific Pte Ltd.

Primary address:

70 Pasir Panjang Road #03-71,
Mapletree Business City II
Singapore, 117371

Web address: https://cloud.google.com

Contact name:

Contact number:

MTCS certificate number:

Company stamp:

Signature of company representative:

DocuSigned by:
Suzanne Frey

DocuSigned by:
Royal Hansen

Certification Body Contact Information

Company name: EY CertifyPoint

Web address: https://www.ey.com/en_gl/advisory/certify-point

Contact name: Jatin Sehgal

Contact email: certifypoint@nl.ey.com

Company stamp:

Signature of lead auditor:

Cloud Service Provider Background

Overview of service offering:

Google Cloud lets you focus on what's next for your business. Google Cloud frees you from the overhead of managing infrastructure, provisioning servers and configuring networks. To let innovators innovate and let coders, well, just code. From Gmail to Docs, Drive, and Calendar, collaborate with Google Cloud anytime, anywhere across your computer, phone, and tablet.

Service model:

☐ Virtual machine instances owned by the user

☐ 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	1. Right to audit	The user has the right to audit: **Virtual machine instances owned by the user** Network facilities Compliance with applicable standards Technical controls Policies and governance Data centre facilities Others _____**right to audit is specific to customer contractual terms** None Regulators recognised by Singapore law have the right to audit: Virtual machine instances owned by the user 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:	Our customers and regulators expect independent verification of security, privacy and compliance controls. Google undergoes several independent third party audits on a regular basis to provide this assurance. This means that an independent auditor has examined the controls present in our data centers, infrastructure and operations. Google's third party audit approach is designed to be comprehensive in order to provide assurances of Google's level of information security with regard to confidentiality, integrity and availability. Customers may use these third party audits to assess how Google's products can meet their compliance and data-processing needs. Google will allow customers or an independent auditor appointed by the Customer to conduct audits to verify

		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) (yes)**	Google's compliance with its obligations under our terms, as indicated in our Data Protection Agreement (section 7.5.2)
2	Compliance	2. 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** **PCI-DSS** Others _____	Google is committed to protecting your organization's data. We undergo several independent third-party audits on a regular basis. For the complete and updated list, please visit https://cloud.google.com/security/compliance Google has provided documentation describing control environment in order to enable customers to evaluate the suitability of Google Cloud within the context of Singapore PDPA: https://cloud.google.com/files/singapore-pdpa-wp.pdf Google reviews the Information Security Policy annually and has processes in place to ensure that Information Security Policies and supporting guidance are current and aligned with the needs of the organization. As such, we believe we are addressing the risk for which clause 6.5.3a is intended. Google performs periodic evaluations of Cloud Service delivery and performs background checks on new hires, where legally permissible. As such, we believe we have addressed the risk for which clause 7.1.4a is intended
Data Control			
3	Data ownership	All data on the cloud service is owned by the cloud user except for:_____	Google does not use customer content for marketing or advertising purposes. Google Cloud may advertise directly to

		_____ The cloud User retains the ownership on the derived data or attributes of cloud usage except for the following: **Advertising or marketing** **Statistics analysis on usage** **Others_Product development**_____ _____	Google Cloud customers to market additional services which may be of interest to those customers.
4	Data retention	Data deleted by the user is retained as follows: Minimum data retention period is: ___**30 days (GCP); 20 days (G Suite)**____ Maximum data retention period is: __**180 days**_____ Deleted immediately Log data is retained for a period of: Minimum data retention period as follows: ____**30 to 400 days (GCP); 30 days to 15 months (G Suite)**____ Maximum data retention period is: ___**30 to 400 days (GCP); 30 days to 15 months (G Suite)**___ Not retained User 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 user: **Log data** **Other** ___any user data_____	Please refer to https://cloud.google.com/terms/data-processing-terms#7-data-correction-blocking-exporting-and-deletion https://cloud.google.com/security/deletion/#deletion_timeline https://support.google.com/a/answer/33314?hl=en https://gsuite.google.com/terms/dpa_terms.html https://cloud.google.com/logging/quotas#logs_retention_periods https://support.google.com/a/answer/7061566 Customers are responsible for logging and monitoring changes in a cloud user's administrators account in accordance with clause 23.8. For Clause 23.8.3, Google has provided Cloud Identity Agreement that states the customer agrees that Google's responsibilities do not extend to the internal management or administration of the services for customers and that Google is merely a data processor. https://cloud.google.com/terms/identity/na_terms
5	Data sovereignty	The primary data locations are: Singapore Asia Pacific _____ Europe_____ United States **Other** _https://cloud.google.com/about/locations/#regions-tab https://gsuite.google.com/security/?secure-by-d	**GCP** For certain Google Cloud Platform services, customers may select where their data will be stored (the "Data Location Selection"), and Google will store it there in accordance with the Service Specific Terms. If a Data Location Selection is not covered by

		esign_activeEl=data-centers___ The backup data locations are: Singapore Asia Pacific_____ Europe_____ United States **Other** _____see above_____ No. of countries in which data centres are operated: _____ The user'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: _____ **No** User'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 users are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. In addition, users 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.	the Service Specific Terms (or a Data Location Selection is not made by Customer in respect of any Customer Data), Google may store and process the relevant Customer Data anywhere Google or its Subprocessors maintains facilities. Google stores data in a multi-tenant environment on Google-owned servers. The data and file system architecture are replicated between multiple geographically dispersed data centers. https://cloud.google.com/about/locations/#regions-tab **G Suite** Per section 1.1 of the G Suite TOS, G Suite, as part of providing the services may transfer, store, and process customer data in countries where Google maintains facilities. To review our current list of datacenter locations where G Suite data is located, please see: https://www.google.com/about/datacenters/inside/locations/index.html Google does not host data at any third party data centers where Google does not own and manage the physical security boundary and control therefore clauses 9.2.4 (a) and 9.4.4 (d) are not applicable to the Google environment.
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)**	Google ensures that a non-disclosure agreement is in place before sharing any confidential information with any customer. Google will also work with the customer if they request to use their NDA template.
Provider Performance			
7	Availability	The committed network uptime is: _____%	https://cloud.google.com/terms/sla/ https://gsuite.google.com/intl/en/terms/

		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	sla.html
8	BCP / DR	Disaster recovery protection Backup and restore service User selectable backup plans Escrow arrangements No BCP / DR is available RPO_____ RTO_____ **Others, please specify:** _____ _____ _____	Google replicates data over multiple locations to help protect against accidental destruction or loss. GCP customers may schedule their own backups using provided services, such as Cloud archival or Cold Storage.
9	Liability	The following terms are available for the users 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:_____ _____ Database failure Liability:_____ _____ Monitoring failure Liability:_____ _____	Google shall use all reasonable commercial efforts to ensure that all the GCP services are operated and available to customers based on the service level agreements described below.. In the event Customer experiences any of the service performance issues defined below due to Google's failure to provide Services, Customer will be eligible to receive the Service Credits described below: https://cloud.google.com/terms/sla/ During the Term of the applicable G Suite Agreement, the G Suite Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month (the ""G Suite SLA""). If Google does not meet the G Suite SLA, and if Customer meets its obligations under this G Suite SLA, Customer will be eligible to receive the Service Credits described below. This G Suite SLA states Customer's sole and exclusive remedy for any failure by

			Google to meet the G Suite SLA. https://gsuite.google.com/intl/en/terms/sla.html
Service Support			
10	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	https://cloud.google.com/terms/tssg/ https://gsuite.google.com/intl/en/terms/standard_terms.html https://gsuite.google.com/intl/en_in/terms/2013/1/premier_terms.html https://gsuite.google.com/intl/en/terms/tssg.html
11	Self-service provisioning and management portal	Provide self-service provisioning and management portal for users 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** Others: _____ ____ _____ _____	Google's self service platform provides users the ability to administer users and manage their Google services. Additionally, Cloud users are able to manage resource pools through the consoles and track usage statistics.
12	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	https://cloud.google.com/support/?options=premium-support#options https://gsuite.google.com/support/

		hours of operations: _____ Service response time: _____ The following are available to users upon request: Permanent access to audit records of customer instances **Incident management assistance** Incident response time: _____ Mean time to repair on detection of faults: _____	
13	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): **Pay per usage _____ (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per user per hour/day/month/year for SaaS)** Fixed pricing_____(up to yearly/monthly/daily) Other pricing model_____ Not disclosed Available billing history: _____Months	Information about Google Cloud & G Suite Pricing may be found at https://cloud.google.com/pricing/ https://gsuite.google.com/pricing.html
14	Data portability	Importable VM formats: _____ Downloadable formats: _____ Supported operating systems: _____ Language versions of supported operating systems: _____ _____ Supported database formats: _____ API: Common _____ _ Customised _____ Upon service termination, data is available through: Physical media **Standard methods as described above** **Other methods**	https://cloud.google.com/migrate/ https://cloud.google.com/solutions/best-practices-migrating-vm-to-compute-engine https://support.google.com/accounts/answer/3024190?hl=en https://cloud.google.com/security/gdpr/ https://takeout.google.com/?pli=1 https://support.google.com/a/answer/100458?hl=en

		_____ _____ _____	
15	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** _____Google Interconnect _____ _____ _____ _____ _____ Public access speed (shared bandwidth) in Mbps: _____ _____	In addition to the methods to the left, Google also offers Interconnect to its GCP customers. https://cloud.google.com/interconnect/ Google Cloud Interconnect allows Google Cloud Platform customers to connect to Google via enterprise-grade connections with higher availability and/or lower latency than their existing Internet connections. Connections are offered by Cloud Interconnect service provider partners, and may offer higher SLAs than standard Internet connections. Google also supports direct connections to its network through direct peering. Customers who cannot meet Google at its peering locations, or do not meet peering requirements, may benefit from Cloud Interconnect. https://cloud.google.com/interconnect/
16	User management	**Identity management** **Role based access control** **Federated access model** **Integration with Identity management solutions** Others_____ _____	Google offers Cloud Identity & Access management that allows administrators to authorize who can take action on specific resources, giving them full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups and potentially many more projects, Cloud IAM provides a unified view into security policy across customer's organization, with built-in auditing to ease compliance processes. https://cloud.google.com/iam/ https://cloud.google.com/identity/ Below MTCS clauses are not applicable: Clause 22.12 is not applicable as third party admins do not have access

			Clause 22.13 is not applicable as service and application accounts are not used https://cloud.google.com/terms/data-processing-terms Google has adopted NIST guidance (SP 800-63c) and, as such, does not enforce password history and rotation requirements as defined in clause 22. Google's password policies provide "equivalent or better security" than the requirements established in clause 22. Google has provided the ability to integrate customer's SSO via SAML, which allows them to configure their password settings to meet MTCS standards. As such, we consider this an alternative implementation to meet the requirements in Clause 23. Clauses 23.2, 23.4.2 (b) and (c), 23.7.2 (b) are not applicable as user access security is a shared responsibility between Google & Customer Additionally, customers are responsible for removing custom applications accounts, user IDs, passwords, test data and accordance in accordance with clauses 16.1.2 (b) and (c). Google employs robust, proprietary services and mechanisms to encrypt G Suite user data, as such, we believe we are addressing the risk for which clause 24.6.4a is intended. Clause 17.1.2a is not applicable as GCP customers can manage the keys themselves by using Cloud KMS or bring their own keys to Google Cloud. Clauses 17.3.3g, h and 17.3.4a are the responsibility of GCP customers to the extent that they utilize our Customer

			Managed Key capability, thereby using Hardware Security Module (HSM). Clauses 17.3.3g, h and 17.3.4a are not applicable for G Suite as Google does not use HSMs for internal key management system (KMS). Cloud Customer Managed Encryption Keys https://cloud.google.com/storage/docs/encryption/customer-managed-keys Cloud HSM https://cloud.google.com/hsm/ G Suite Key Management https://services.google.com/fh/files/helpcenter/google_encryptionwp2016.pdf Please refer to Google's Encryption at Rest in Google Cloud Platform security whitepaper for additional information. https://cloud.google.com/security/encryption-at-rest/default-encryption/
17	Lifecycle	The cloud user may select the following for service upgrades and changes: **Automatic provisioning** User customisable provisioning	https://cloud.google.com/identity/solutions/automate-user-provisioning
Security Configurations			
18	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? _____ _____	https://cloud.google.com/terms/data-processing-terms#7-data-correction-blocking-exporting-and-deletion https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures https://gsuite.google.com/terms/dpa_terms.html
19	Multi-tenancy	Distinct physical hosts Distinct physical network infrastructure **Virtual instance grouping** **User definable security domains**	

		User customisable firewall **User definable access policies**	
Service Elasticity			
20	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** ____2TB_____ **(number of cores and GB memory)**	Google's Instance groups offer GCP customers managed groups that can automatically scale the number of instances in the group, work with load balancing services to distribute traffic to all of the instances in the group and automatically recreate the instance in the event of an incident. In addition to the automatic load balancing, Google also offers Health Checks that checks the health of the instance and the server. https://cloud.google.com/compute/docs/instance-groups/ https://cloud.google.com/compute/docs/load-balancing/health-checks
21	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: _____ _____ _____ _____ _____ Network traffic isolation, please specify: _____ _____ _____ 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 _____	
22	Storage redundancy and 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 user, please specify: _____ _____ Maximum expandable storage, please specify: _____ _____ **Alerts to be sent for unusual high usage** Minimum storage I / O performance during peak periods _____ _____ Minimum period to scale up storage I / O throughput _____ _____	Google offers various storage options to customers based on their needs (https://cloud.google.com/storage/) https://support.google.com/googlecloud/answer/6056635?hl=en&ref_topic=6055719 MTCS Standard, Clause 24.5 is not applicable.