

Cloud Service Provider Contact Information

Company Name: Google Asia Pacific Pte Ltd
Primary Address: 70 Pasir Panjang Road, #03-71, Mapletree Business City, Singapore 117371
Web Address: <https://cloud.google.com>
Contact Name: [Christopher Johnson](#)

Cloud Service Provider Background

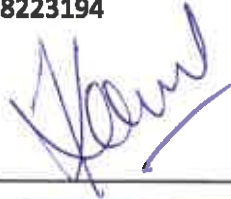
Google Cloud lets you focus on what's next for your business. Google Cloud frees you from the overhead of managing infrastructure, provisioning servers and configuring networks. To let innovators innovate and let coders, well, just code. From Gmail to Docs, Drive, and Calendar, collaborate with Google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

Service Model SaaS (G Suite) PaaS and IaaS (GCP)
Deployment model Public Cloud
Tier Level MTCS Level 3
Remark

Certificate Number

Certification Body Contact Information

Company name: TUV SUD PSB Pte Ltd
Web address: www.tuv-sud-psb.sg
Contact name: Nur Kamal Bin kamari
Contact number: 88223194



Company Stamp & Signature:

TÜV SÜD PSB Pte Ltd
1 Science Park Drive
Singapore 118221
Tel : +65 6778 7777 Fax : +65 6779 7088
Co. Reg. No. : 199002667R

Compliance

Right to audit	<p>The user has the right to audit:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Virtual machine instances owned by the user <input type="checkbox"/> Network facilities <input checked="" type="checkbox"/> Compliance with applicable standards <input type="checkbox"/> Technical controls <input checked="" type="checkbox"/> Policies and governance <input type="checkbox"/> Data centre facilities <input type="checkbox"/> Others <input type="checkbox"/> None <p>Regulators recognised by Singapore law have the right to audit:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Virtual machine instances owned by the user <input type="checkbox"/> Network facilities <input checked="" type="checkbox"/> Compliance with applicable standards <input checked="" type="checkbox"/> Technical controls <input checked="" type="checkbox"/> Policies and governance <input type="checkbox"/> Data centre facilities <input type="checkbox"/> Others <input type="checkbox"/> None <p>Audit / assessment reports that can be made available on request:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Penetration test <input type="checkbox"/> Threat and vulnerability risk assessment <input type="checkbox"/> Vulnerability scan <input checked="" type="checkbox"/> Audit reports (e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation) 	<p>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.</p>
-----------------------	--	---

Compliance	<p>The following guidelines / standards / regulations are adhered to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Singapore Personal Data Protection Act <input checked="" type="checkbox"/> ISO / IEC 27001 <input type="checkbox"/> ISO 9000 <input type="checkbox"/> ISO / IEC 20000 	<p>More information about the latest compliance programs and certifications can be found at https://cloud.google.com/security/compliance</p>
-------------------	---	---

- CSA STAR
- PCI-DSS
- Others

and <https://gsuite.google.com/security/>

Data Control

Data ownership

All data on the cloud service is owned by the cloud user except for:
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

Data retention

Data deleted by the user is retained as follows:

- Minimum data retention period is:
- Maximum data retention period is: 180 Days
- Deleted immediately

Log data is retained for a period of:

- Minimum data retention period as follows: _____
- Maximum data retention period is: 180 Days
- Not retained

User data is retained for a period of:

- Minimum data retention period is: _____
- Maximum data retention period is: per our Cloud Terms of Service, data may be retained up to 180 days after account termination
- Not retained

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

- Log data

Per our Terms of Service (<https://cloud.google.com/terms/data-processing-terms#7-data-correction-blocking-exporting-and-deletion>): During the Term, Google will provide Customer with the ability to correct, block, export and delete Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Customer deletes Customer Data via the Services such that the Customer Data cannot be recovered by Customer (the "Customer-Deleted Data"), Google will delete the Customer-Deleted Data within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so. On

Other

the expiry or termination of the Agreement (or, if applicable on expiry of any post-termination period during which Google may agree to continue providing access to the Services), after a recovery period of up to 30 days following such expiry or termination, Google will thereafter delete the Customer-Deleted Data within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

GSuite DPA

DPA:

https://gsuite.google.com/terms/dpa_terms.html

7.1. Deletion by Customer and End Users. During the Term, Google will provide Customer or End Users with the ability to delete Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Customer or End User deletes Customer Data and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash" ("Customer-Deleted Data"), Google will delete such data from its systems as soon as reasonably practicable within a maximum period of

Data sovereignty The primary data locations are:

- Singapore
- Asia Pacific
- Europe

Per our Terms of Service (<https://cloud.google.com/terms/data-processing-terms#7-data-correction-blocking-exporting-and-deletion>): During the Term, Google will provide Customer with the ability

United States

Other

The backup data locations are:

Singapore

Asia Pacific

Europe

United States

Other

No. of countries in which data centres are operated: 11

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:: G Suite users may not chose the location of SaaS cloud data

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: The G Suite products may automatically backup to other datacenter to retain performance and availability

No

Note: Cloud users are responsible for determining the impact of data protection and data sovereignty.....

Google will provide Customer with the ability to correct, block, export and delete Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Customer deletes Customer Data via the Services such that the Customer Data cannot be recovered by Customer (the "Customer-Deleted Data"), Google will delete the Customer-Deleted Data within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so. On the expiry or termination of the Agreement (or, if applicable on expiry of any post-termination period during which Google may agree to continue providing access to the Services), after a recovery period of up to 30 days following such expiry or termination, Google will thereafter delete the Customer-Deleted Data within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

GSuite DPA

DPA:

https://gsuite.google.com/terms/dpa_terms.html

7.1. Deletion by Customer and End Users. During the Term, Google will provide

Non-disclosure

Non-disclosure agreement template can be provided by Cloud Service Provider

Cloud Service Provider may use customer's NDA (pending legal review)

Provider Performance

Availability

For each cloud service offered, CSP should disclose relevant numbers)

The committed network uptime is:

Varies according to price plan

The committed system uptime is:

SLAs are described in the service specific Terms of Service.

<https://cloud.google.com/terms/sla/>

https://gsuite.google.com/terms/partner_sla.html

varies according to price plan

The cloud environment has the following single points of failure:

None

Disaster recovery protection

BCP / DR

Backup and restore service

User selectable backup plans

Escrow arrangements

No BCP / DR is available

RPO

RTO

Others, please specify:

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

Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

Liability:

Service Support

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

Self-service provisioning and management portal

Provide self-service provisioning and management portal for users to manage cloud services:

Yes

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:

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: _____

Google Cloud has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800-61). Key staff are trained in

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: _____

forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team.

Billing

The following billing modes are available (please elaborate granularity of charges and measurements)

- Pay per usage minute on some services (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per user per hour/day/month/year for SaaS)
- Fixed price _____ up to yearly/monthly/daily
- Other pricing model
- Not disclosed
- Available billing history: _____ Months

Information about Google Cloud Pricing may be found at <https://cloud.google.com/pricing>

Data portability

Importable VM formats: Multiple

Downloadable formats: _____

Supported operating systems: _____

Language versions of supported operating systems: _____

Supported database formats: _____

API:

- Common _____

<https://cloud.google.com/migrate/>

<https://cloud.google.com/solutions/best-practices-migrating-vm-to-compute-engine>

Customised _____

Upon service termination, data is available through:

- Physical media
- Standard methods as described above
- Other methods

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:

In addition to the methods to the left, Google Cloud also offers Interconnect. <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.

User management

- Identity management
- Role based access control
- Federated access model
- Integration with Identity management solutions
- Others

Lifecycle

The cloud user may select the following for service upgrades and changes:

- Automatic provisioning
- User customisable provisioning

configuration configuration

Security configuration enforcement checks are performed:

- Manually
- Using automated tools

How often are enforcement check being performed to ensure all security configurations are applied?

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

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 _____ (number of cores and GB memory)

[Managed instance groups](#) offer autoscaling capabilities that allow you to automatically add or remove instances from a managed instance group based on increases or decreases in load. Autoscaling helps your applications gracefully handle increases in traffic and reduces cost when the need for resources is lower. You just define the [autoscaling policy](#) and the autoscaler performs automatic scaling

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 Mbps

NA

Maximum usable IPs _____

NA

- Load Balancing Ports
- Load balancing protocols
- Anti-DDOS protection systems or services
- Defence-in-depth mechanisms, please specify: _____
- Network traffic isolation, please specify: _____

<https://cloud.google.com/beyondcorp/>

<https://cloudplatform.googleblog.com/2014/04/enter-andromeda-zone-google-cloud-platforms-latest-networking-stack.html>

<input type="checkbox"/>	Shared or dedicated bandwidth, please specify: _____	
<input checked="" type="checkbox"/>	QoS traffic control services	
<input checked="" type="checkbox"/>	Alerts to be sent for unusual high usage	
<input type="checkbox"/>	Minimum performance during peak periods	NA
<input type="checkbox"/>	Minimum period to scale up network throughput _____	NA

Storage redundancy and elasticity		
The following storage redundancy and elasticity options are available:		
<input checked="" type="checkbox"/>	Redundant storage connectivity links within each data centre	
<input checked="" type="checkbox"/>	Redundant storage connectivity links between data centres belonging to the same cloud	
<input type="checkbox"/>	Storage traffic isolation, please specify: _____	
<input type="checkbox"/>	Shared or dedicated storage network bandwidth, please specify:	
<input checked="" type="checkbox"/>	Quality of service storage traffic control services	
<input type="checkbox"/>	Maximum storage capacity for entire cloud, please specify:	NA
<input type="checkbox"/>	Maximum storage capacity for single user, please specify:	NA
<input type="checkbox"/>	Maximum expandable storage, please specify:	NA
<input checked="" type="checkbox"/>	Alerts to be sent for unusual high usage	
<input type="checkbox"/>	Minimum storage I / O performance during peak periods	NA
<input type="checkbox"/>	Minimum period to scale up storage I / O throughput	NA