



---

**System and Organization Controls (SOC) 3  
Report on the Google Cloud Platform System  
Relevant to Security, Availability, and Confidentiality  
For the Period 1 November 2018 to 31 October 2019**

---



Google LLC  
1600 Amphitheatre  
Parkway  
Mountain View, CA, 94043

650 253-0000 main  
Google.com

**Management's Report of its Assertions on the Effectiveness of Controls  
Over the Google Cloud Platform  
Based on the Trust Services Criteria for Security, Availability, and  
Confidentiality**

We, as management of, Google LLC ("Google" or "the Company") are responsible for:

- Identifying the Google Cloud Platform (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the Google Cloud Platform (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period 1 November 2018 to 31 October 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

**Google LLC**  
18 December 2019

## **Report of Independent Accountants**

To the Management of Google LLC:

### *Scope*

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls over the Google Cloud Platform System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality" (Assertion), that Google's controls over the Google Cloud Platform (System) were effective throughout the period 1 November 2018 to 31 October 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

### *Management Responsibilities*

Google's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Google Cloud Platform (System) and describing the boundaries of the System
- Identifying its principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of its system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Google Cloud Platform (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements

### *Our Responsibilities*

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Google's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.



Our examination was not conducted for the purpose of evaluating Google's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

*Inherent limitations*

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Google's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

*Opinion*

In our opinion, Google's controls over the system were effective throughout the period 1 November 2018 to 31 October 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

*Ernst & Young LLP*

18 December 2019  
San Jose, CA

## Attachment A – Google Cloud Platform System

### Google Cloud Platform System

Google LLC ("Google" or "the Company") is a global technology service provider focused on improving the ways people connect with information. Google's innovations in web search and advertising have made Google's website one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world's largest online index of websites and other content, and makes this information freely available to anyone with an Internet connection. Google's automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Google Cloud Platform provides Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), allowing businesses and developers to build and run any or all of their applications on Google's Cloud infrastructure. Customers can benefit from performance, scale, reliability, ease-of-use, and a pay-as-you-go cost model.

Google Cloud Platform includes the following services, hereafter described collectively as "Google Cloud Platform" or GCP:

#### AI and Machine Learning

- AutoML Tables\*
- AI Platform Training and Prediction
- AI Platform Notebooks\*
- Cloud AutoML Natural Language
- Cloud AutoML Translation
- Cloud AutoML Video\*
- Cloud AutoML Vision
- Cloud Natural Language
- Cloud Speech-to-Text
- Cloud Text-to-Speech
- Cloud Translation
- Cloud Video Intelligence
- Cloud Vision
- Dialogflow Enterprise Edition

#### Compute

- App Engine
- Cloud Functions
- Cloud Functions for Firebase\*
- Cloud Run\*
- Compute Engine
- Kubernetes Engine

## Data Analytics

- BigQuery
- BigQuery Data Transfer Service
- Cloud Dataflow
- Cloud Datalab
- Cloud Dataproc
- Cloud Pub/Sub
- Data Catalog\*
- Cloud Life Sciences

## Developer Tools

- Cloud Build
- Cloud SDK
- Cloud Source Repositories
- Container Registry

## Identity and Security

- Access Context Manager\*
- Access Transparency
- Cloud HSM
- Cloud Identity and Access Management
- Cloud Identity-Aware Proxy
- Cloud Key Management Service
- Cloud Resource Manager
- Cloud Security Scanner
- Data Loss Prevention
- Firebase Authentication\*
- Google Service Control
- Identity Platform
- VPC Service Control\*

## Management Tools

- Cloud Console
- Cloud Console Mobile App
- Cloud Deployment Manager
- Cloud Shell
- Stackdriver Debugger
- Stackdriver Error Reporting
- Stackdriver Logging
- Stackdriver Profiler
- Stackdriver Trace

## Networking

- Google Cloud Armor
- Cloud CDN
- Cloud DNS
- Cloud Interconnect
- Cloud Load Balancing
- Cloud NAT\*
- Cloud Router
- Cloud VPN
- Network Service Tiers
- Virtual Private Cloud (VPC)

## Storage and Databases

- Cloud Bigtable
- Cloud Datastore
- Cloud Filestore
- Cloud Firestore
- Cloud Memorystore
- Cloud Spanner
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase\*
- Cloud Storage Transfer Service
- Persistent Disk

## Other

- Cloud Billing API
- Cloud Endpoints
- Cloud Healthcare
- Cloud Healthcare Search
- Cloud IoT Core
- Cloud Talent Solution
- Firebase Test Lab\*
- GCP Marketplace
- Google Service Management
- Orbitera
- Service Consumer Management

\*Indicates products in scope for the period 1 May 2019 through 31 October 2019

Google's product offerings for Google Cloud Platform provide the unique advantage of leveraging the resources of Google's core engineering team while also having a dedicated team to develop solutions for the corporate market. As a result, these Google offerings are positioned to innovate at a rapid rate and provide the same level of service that users are familiar with on google.com.

These products provide a comprehensive variety of technical services that organizations rely on:

- AI and Machine Learning - fast, scalable and easy to use modern machine learning services, with pre-trained models and the ability to generate tailored models
- Compute - a scalable range of computing options tailored to match the size and needs of an organization
- Data Analytics - tools to capture, process, store and analyze data on a single platform
- Developer Tools - a rich collection of tools and libraries that help development teams work quickly and effectively
- Identity and Security - manage the security and access to cloud assets, supported by Google's own protection of its infrastructure
- Management Tools - manage apps on GCP with a web-based console, mobile app, or Cloud Shell for real time monitoring, logging, diagnostics, and configuration
- Networking - a high quality private network using software-defined networking and distributed systems technologies to host and deliver services around the world
- Storage and Databases - scalable storage options and varieties for different needs and price points

The products are comprised of communication, productivity, collaboration and security tools that can be accessed from virtually any location with Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with an Internet connection.

The Google Cloud Platform products covered in this system description consist of the following services:

## **AI and Machine Learning**

### *AutoML Tables*

AutoML Tables enables data scientists, analysts, and developers to automatically build and deploy machine learning models on structured data at increased speed and scale.

### *AI Platform Training and Prediction*

AI Platform Training and Prediction is a managed service that enables users to easily build machine learning models with popular frameworks like TensorFlow, XGBoost and Scikit Learn. It provides scalable training and prediction services that work on large datasets.

### *AI Platform Notebooks*

AI Platform Notebooks is a semi-managed service that offers integration with JupyterLab environments in which machine learning developers and data scientists can create running instances with data science and machine learning frameworks in a single click.

### *Cloud AutoML Natural Language*

AutoML Natural Language enables categorization of input text into their own custom defined labels (supervised classification). Models can be specific for a domain or use case.



### *Cloud AutoML Translation*

Cloud AutoML Translation enables training of custom models with limited machine learning expertise so translation queries return results specific to their domain. After uploading translated language pairs, AutoML Translation will train and deploy a model that can scale as needed to meet production demands. AutoML Translation offers the ability to create a production-ready model in a short amount of time.

### *Cloud AutoML Video*

Cloud AutoML Video delivers a simple and flexible machine learning service that lets businesses and customer developers train custom and scalable video models for specific domain or use cases.

### *Cloud AutoML Vision*

Cloud AutoML Vision enables training of custom models to classify images according to defined labels. After uploading and labeling images, Cloud AutoML Vision will train a model and manage deployment to adapt to demands. Cloud AutoML Vision offers high model accuracy and fast time to create a production-ready model. It also supports models to detect objects in images, and download classification-only models for use on edge devices.

### *Cloud Natural Language*

Cloud Natural Language provides natural language understanding as a simple to use Application Programming Interface (API). Given a block of text, this API enables finding entities, analyzing sentiment (positive or negative), analyzing syntax (including parts of speech and dependency trees), and categorizing the content into a rich taxonomy. The API can be called by passing the content directly or by referring to a document in Google Cloud Storage.

### *Cloud Speech-to-Text*

Cloud Speech-to-Text allows converting audio to text by applying neural network models in an API. The API can recognize over 80 languages and variants. Users can transcribe the text of users dictating to an application's microphone, enable command-and-control through voice, or transcribe audio files, among many other use cases. The API can receive streamed audio or a URL to audio stored in Google Cloud Storage.

### *Cloud Text-to-Speech*

Google Cloud Text-to-Speech synthesizes natural-sounding speech with 30 voices, available in multiple languages and variants to deliver high fidelity audio, creating lifelike interactions across many applications and devices.

### *Cloud Translation*

Cloud Translation automatically translates text from one language to another language (e.g., French to English). The API is used to programmatically translate text in webpages or apps.

### *Cloud Video Intelligence*

Cloud Video Intelligence API makes videos searchable, and discoverable, by extracting metadata through a REST API. It annotates videos stored in Google Cloud Storage, and helps identify key noun entities in a video and when they occur within the video.

### *Cloud Vision*

Cloud Vision enables the understanding of image content by encapsulating machine learning models in a REST API. It classifies images into thousands of categories, detects individual objects and faces within images, and finds and reads printed words contained within images. It can be applied to build metadata on image catalogs, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. It can also analyze images uploaded in the request and integrate with image storage on Google Cloud Storage.

### *Dialogflow Enterprise Edition*

Dialogflow is a development suite for voice and text conversational apps including chatbots. Dialogflow is cross-platform and can connect to apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).

## **Compute**

### *App Engine*

App Engine enables the building and hosting of web apps on the same systems that power Google applications. App Engine offers fast development and deployment. There is no need to manage servers or other low-level infrastructure components. Scaling and software patching are handled by App Engine on the user's behalf. App Engine also provides the ability to create managed VMs. In addition, client APIs can be built for App Engine applications using Google Cloud Endpoints.

### *Cloud Functions*

Cloud Functions is a serverless compute solution that runs single-purpose functions in response to GCP events and HTTP calls (webhooks). Cloud Functions can be triggered asynchronously by Cloud Pub/Sub, Cloud Storage, GCP infrastructure events, and Firebase products. Cloud Functions scales automatically to meet request load and the user does not need to manage servers or the runtime environment.

### *Cloud Functions for Firebase*

Cloud Functions for Firebase are developer tools used for development and deployment of Google Cloud Functions. Cloud Functions enable developers to run their own backend code that executes automatically based on HTTP requests and Firebase and Google Cloud Platform events. Developers functions are stored in Google's cloud and run in a managed Node.js environment.

### *Cloud Run*

Cloud Run is a fully managed compute platform that automatically scales stateless HTTP containers, running requests or event-driven stateless workloads.

### *Compute Engine*

Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud. With virtual machines that can boot in minutes, it offers many configurations including custom machine types that can be optimized for specific use cases as well as support for Graphics Processing Units (GPUs), Tensor Processing Units (TPUs) and Local SSD. Additionally, customers can enable Shielded VMs to provide advanced platform security.

### *Kubernetes Engine*

Kubernetes Engine, powered by the open source container scheduler Kubernetes, runs containers on Google Cloud Platform. Kubernetes Engine manages provisioning and maintaining the underlying virtual machine cluster, scaling applications, and operational logistics such as logging, monitoring, and cluster health management.

## **Data Analytics**

### *BigQuery*

BigQuery is a fully managed data analysis service that features scalable data storage, up to hundreds of terabytes, the ability to perform ad hoc queries on multi-terabyte datasets, and the ability to share data insights via the web.

### *BigQuery Data Transfer Service*

BigQuery Data Transfer Service automates data movement from Software as a Service (SaaS) applications to BigQuery on a scheduled, managed basis.

### *Cloud Dataflow*

Cloud Dataflow is a fully managed service for consistent, parallel data-processing pipelines. It utilizes the Apache Beam Software Development Kits (SDKs) with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the lifecycle of Compute Engine resources for the processing pipeline(s), and provides a monitoring interface for understanding pipeline health.

### *Cloud Datalab*

Cloud Datalab is an interactive notebook based tool for exploration, transformation, analysis and visualization of data on Google Cloud Platform. It provides analytical and storage services to analyze data on the platform.

### *Cloud Dataproc*

Cloud Dataproc is a managed service for distributed data processing. It provides management, integration, and development tools for deploying and using Apache Hadoop, Apache Spark, and other related open source data processing tools. With Cloud Dataproc, clusters can be created and deleted on-demand and sized to fit whatever workload is at hand.

### *Cloud Pub/Sub*

Cloud Pub/Sub provides reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a topic while other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Google Cloud Pub/Sub allows communication between independent applications.

### *Data Catalog*

Data Catalog is a fully managed and scalable metadata management service that allows organizations to have a centralized and unified view of data assets.

### *Cloud Life Sciences*

Cloud Life Sciences provides an API to store, process, inspect and share DNA sequence reads, reference-based alignments, and variant calls, using Google's cloud infrastructure.

## **Developer Tools**

### *Cloud Build*

Cloud Build allows for the creation of container images from application source code located in Google Cloud Storage or in a third party service (e.g., Github, Bitbucket). Created Container images can be stored in Container Registry and deployed on Container Engine, Compute Engine, App Engine Flexible Environment or other services to run applications from Docker containers.

### *Cloud SDK*

Cloud SDK is a set of command-line tools for the Google Cloud Platform that can be run interactively or in automated scripts. These tools can be used to manage supported Google Cloud Platform products, including Compute Engine virtual machines, Kubernetes clusters, network and firewall configurations, and disk storage.

### *Cloud Source Repositories*

Cloud Source Repositories provides Git version control to support collaborative development of any application or service as well as a source browser that can be used to browse the contents of repositories and view individual files from within the Cloud Console. Cloud Source Repositories and related tools (e.g., Stackdriver Debugger) can be used to view debugging information alongside code during application runtime.

### *Container Registry*

Container Registry is a private Docker image storage system on Google Cloud Platform.

## **Identity and Security**

### *Access Context Manager*

Access Context Manager allows customer administrators to define attribute-based access control for projects, apps and resources.

### *Access Transparency*

Access Transparency captures near real-time logs of certain manual, targeted accesses by Google personnel, and provides them via Stackdriver Logging accounts.

### *Cloud HSM*

Cloud HSM is a cloud-hosted Hardware Security Module (HSM) service for hosting encryption keys and performing cryptographic operations.

### *Cloud Identity and Access Management*

Cloud Identity and Access Management (IAM) enables the administration and authorization of accesses to specific resources, and provides a unified view into security policies across entire organizations with built-in auditing.

### *Cloud Identity-Aware Proxy*

Cloud Identity-Aware Proxy (Cloud IAP) is a tool that helps control access to applications running on Google Cloud Platform based on identity and group membership.

### *Cloud Key Management Service*

Cloud Key Management Service (KMS) is a cloud-hosted key management service that manages encryption for cloud services. It enables the generation, use, rotation, and destruction of encryption keys.

### *Cloud Resource Manager*

Cloud Resource Manager allows users to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects) to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization enables users to management of common aspects of resources such as access control and configuration settings.

### *Cloud Security Scanner*

Cloud Security Scanner is a web application security scanner for Google App Engine. It provides the ability to check for a subset of common web application vulnerabilities in websites built on App Engine.

### *Data Loss Prevention*

Cloud Data Loss Prevention (DLP) enables classifying, redacting, and analyzing sensitive or personally identified content in text, images, and cloud assets.

### *Firebase Authentication*

Firebase Authentication is a fully managed user identity and authentication system providing backend services enabling sign-in and sign-up experiences for an application or service.

### *Google Service Control*

Google Service Control provides control plane functionality to managed services, such as logging, monitoring, and status checks.

### *Identity Platform*

Identity Platform is a customer identity and access management (CIAM) platform delivered by Google Cloud enabling organizations to add identity management and user security to their applications or services.

### *VPC Service Control*

VPC Service Control provides administrators with the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized virtual private cloud (VPC) networks.

## **Management Tools**

### *Cloud Console*

Cloud Console is a web-based interface used to build, modify, and manage services and resources on the Google Cloud Platform. Cloud services can be procured, configured, and run from Cloud Console.

### *Cloud Console Mobile App*

Cloud Console Mobile App is a native mobile app that provides monitoring, alerting, and the ability to take actions on resources.

### *Cloud Deployment Manager*

Deployment Manager is an infrastructure management service which automates creation, and management of Google Cloud Platform resources.

### *Cloud Shell*

Cloud Shell provides command-line access to Google Cloud Platform resources through an in-browser Linux shell backed by a temporary Linux VM in the cloud. It allows projects and resources to be managed without having to install additional tools on systems and comes equipped and configured with common developer tools such as text editors, a MySQL client and Kubernetes.

### *Stackdriver Debugger*

Stackdriver Debugger provides the ability to inspect the call-stack and variables of a running cloud application in real-time without stopping it. It is safe to use in test, production or any other deployment environment. It can be used to debug applications written in any programming language.

### *Stackdriver Error Reporting*

Stackdriver Error Reporting counts, analyzes and aggregates the crashes in applications. The crash data is extracted from application logs on Google Cloud or reported via the public API.

Collected data can be inspected via the user interface (UI) or the public API and may opt-in to receive notifications about the occurrence of errors.

### *Stackdriver Logging*

Stackdriver Logging is a fully-managed service that provides a service to store, search, analyze, monitor, and alert of log data and events from Google Cloud Platform and Amazon Web Services (AWS). The API also allows ingestion of custom log data from any source. Stackdriver Logging can ingest application and system log data from thousands of VMs and analyze log data in real-time. Software related to Stackdriver Logging (i.e. open-source logging agent) that can be downloaded and installed on independent VMs is out of the scope of this report.

### *Stackdriver Profiler*

Stackdriver Profiler continuously gathers and reports source-level performance information from production services. It provides key information to determine what functions in code consume the most memory and CPU cycles so insights can be gained on how code operates to improve performance and optimize computing resources.

### *Stackdriver Trace*

Stackdriver Trace collects latency data from applications and displays it in the Google Cloud Platform Console. It automatically analyzes trace data to generate in-depth performance reports that help identify and locate performance bottlenecks.

## **Networking**

### *Google Cloud Armor*

Google Cloud Armor provides access control configurations and at-scale defenses against application-aware and multi-vector attacks.

### *Cloud CDN*

Cloud CDN (Content Delivery Network) uses Google's distributed edge points of presence to cache HTTP(S) load balanced content.

### *Cloud DNS*

Cloud DNS is a fully-managed Domain Name System (DNS) service which operates a geographically diverse network of high-availability authoritative name servers. Cloud DNS provides a service to publish and manage DNS records for applications and services.

### *Cloud Interconnect*

Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform. This solution provides direct connection between on-premise networks and GCP Virtual Private Cloud.

### *Cloud Load Balancing*

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP(S), TCP/SSL, and UDP) to computing resources. Cloud Load Balancing rapidly responds to changes in traffic, network, backend health and other related conditions.

### *Cloud NAT*

Cloud Network Address Translation (NAT) enables virtual machine instances in a private network to communicate with the Internet, without external IP addresses.

### *Cloud Router*

Google Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between a VPC network and an external network, typically an on-premise network.

### *Cloud VPN*

Cloud VPN provides connections between on-premise or other external networks to Virtual Private Clouds on GCP via an IPsec connection or can be used to connect two different Google managed VPN gateways.

### *Network Service Tiers*

Network Service Tiers enable the selection of different quality networks (tiers) for outbound traffic to the Internet: Standard Tier primarily utilizes third party transit providers while Premium Tier leverages Google's private backbone and peering surface for egress.

### *Virtual Private Cloud (VPC)*

Virtual Private Cloud is a comprehensive set of managed networking capabilities including granular IP address range selection, routes and firewalls.

## **Storage and Databases**

### *Cloud Bigtable*

Cloud Bigtable is a low-latency, fully managed, highly-scalable NoSQL database service. It is designed for the retention and serving of data from gigabytes to petabytes in size.

### *Cloud Datastore*

Cloud Datastore is a highly-scalable NoSQL database for mobile and web applications. It provides query capabilities, atomic transitions, indexes, and automatically scales up and down in response to load.

### *Cloud Filestore*

Cloud Filestore is a service for fully managed Network File System (NFS) file servers for use with applications running on Compute Engine virtual machines (VMs) instances or Google Kubernetes Engine clusters.

### *Cloud Firestore*

Cloud Firestore is a fully managed, scalable, serverless NoSQL document database for mobile, web, and server development. It provides query capabilities, live synchronization and offline support.



### *Cloud Memorystore*

Cloud Memorystore for Redis provides a fully managed in-memory data store service for GCP. Cloud Memorystore can be used to build application caches that provides low latency data access. Cloud Memorystore is compatible with the Redis protocol, allowing seamless migration with no code changes.

### *Cloud Spanner*

Cloud Spanner is a fully managed, scalable, relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and ACID (Atomicity, Consistency, Isolation, Durability) transactions with synchronous replication of data across regions.

### *Cloud SQL*

Cloud SQL is a service to create, configure, and use managed third-party relational databases in Google Cloud Platform. Cloud SQL maintains, manages, and administers those databases.

### *Cloud Storage*

Cloud Storage is Google Cloud Platform's unified object/blob storage. It is a RESTful service for storing and accessing data on Google Cloud Platform's infrastructure. It combines the simplicity of a consistent API and latency across different storage classes with reliability, scalability, performance and security of Google Cloud Platform.

### *Cloud Storage for Firebase*

Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for Firebase apps. Cloud Storage for Firebase is backed by Google Cloud Storage, a service for storing and accessing data on Google's infrastructure.

### *Cloud Storage Transfer Service*

Cloud Storage Transfer Service provides the ability to import large amounts of online data into Google Cloud Storage. It can transfer data from Amazon Simple Storage Service (Amazon S3) and other HTTP/HTTPS locations as well as transfer data between Google Cloud Storage buckets.

### *Persistent Disk*

Persistent Disk provides a persistent virtual disk for use with Google Compute Engine and Google Kubernetes Engine compute instances. It is available in both SSD (Solid State Drive) and HDD (Hard Disk Drive) variations.

## **Other**

### *Cloud Billing API*

Cloud Billing API provides methods to programmatically manage billing for projects on the Google Cloud Platform.

### *Cloud Endpoints*

Google Cloud Endpoints is a tool that provides services to develop, deploy, secure and monitor APIs running on Google Cloud Platform.

### *Cloud Healthcare*

Cloud Healthcare provides managed services and an API to store, process, manage, and retrieve healthcare data in a variety of industry standard formats.

### *Cloud Healthcare Search*

Cloud Healthcare Search is a clinician-focused search engine over a patient's longitudinal record. The product offers comprehensive search across all resources in the record along with query expansion, suggest, and spell correction. The externally-accessible provider-facing user interface is vendor-neutral and can be used directly or embedded within an electronic health record system.

### *Cloud IoT Core*

Cloud IoT Core is a fully managed service that securely connects, manages, and ingests data from Internet connected devices. It enables utilization of other Google Cloud Platform services for collecting, processing, and analyzing IoT data.

### *Cloud Talent Solution*

Cloud Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience. The solution includes both Job Search and Profile Search features to provide candidates and employers with an enhanced talent acquisition experience.

### *Firebase Test Lab*

Firebase Test Lab provides cloud-based infrastructure for testing apps on physical and virtual devices. Developers can test their apps across a wide variety of devices with Firebase Test Lab.

### *GCP Marketplace*

Google Cloud Platform (GCP) Marketplace offers ready-to-go development stacks, solutions, and services from 3rd party partners and Google to accelerate development. It enables the deployment of production-grade solutions, obtains direct access to partner support, and receives a single bill for both GCP and 3rd party services.

### *Google Service Management*

Service Management API provides methods for publishing managed services and managing service configurations.

### *Orbitera*

Orbitera provides a platform that creates marketplaces to sell solutions, import billing data and generate reports and invoices, and create time-bound multi-cloud software trials.

### *Service Consumer Management*

Service Consumer Management API provides utilities to help managed service producers manage relationships with service consumers, including the ability to create and manage tenancy units.

### **Data Centers**

The above products are serviced from data centers operated by Google around the world. Below is a list of Google's production data center locations that host the above products and operations for Google Cloud Platform:

- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Lenoir (NC), United States of America
- Moncks Corner (SC), United States of America
- Pryor Creek (OK), United States of America
- Quilicura, Santiago, Chile
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Arcola (VA), United States of America
- Osasco, Brazil
- Montreal, Quebec, Canada
- Los Angeles (CA), United States of America
- Salt Lake City (UT), United States of America
- Clarksville (TN), United States of America
- Widows Creek (AL), United States of America
- Dublin, Ireland
- Eemshaven, Groningen, The Netherlands
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- London (1), United Kingdom
- London (2), United Kingdom
- Frankfurt (1), Hesse, Germany
- Frankfurt (3), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Zurich, Switzerland
- Changhua, Taiwan
- Wenya, Singapore
- Koto-ku, Tokyo, Japan

- Osaka, Japan
- Mumbai, India
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Hong Kong, Hong Kong
- Seoul, South Korea

## **Infrastructure**

Google Cloud Platform runs in a multi-tenant, distributed environment. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Google Cloud Platform, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large distributed databases, built on top of this file system.

## **Data Centers and Redundancy**

Google maintains consistent policies and standards across all data centers for physical security to help protect production and corporate servers, network devices and network connections within Google data centers.

Redundant architecture exists such that data is replicated in real-time to at least two (2) geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

## **Authentication and Access**

Strong authentication and access controls are implemented to restrict access to Google Cloud Platform production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Data traffic is encrypted between Google production facilities.

Google follows a formal process to grant or revoke employee access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system which utilizes Secure Shell (SSH) and TLS certificates help provide secure and flexible access mechanisms. These mechanisms are designed to grant access rights to systems and data only to authorized users.

Both user and internal access to customer data is restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user account ID, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices and support tools is managed

via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semiannual basis under the direction of the group administrators.

## **Change Management**

Change Management policies, including security code reviews and emergency fixes, are in place, and procedures for tracking, testing, approving, and validating changes are documented. Changes are developed utilizing the code versioning tool to manage source code, documentation, release labeling and other functions. Google requires all code changes to be reviewed and approved by a separate technical resource, other than the developer, to evaluate quality and accuracy of changes. Further, all application and configuration changes are tested prior to migration to production environment. Following successful tests, multiple binaries are then grouped into a release and deployed to production.

## **Data**

Google provides controls at each level of data storage, access, and transfer. Google has established training programs for privacy and information security to support data confidentiality. All employees are required to complete these training programs annually. All product feature launches that include new collection, processing, or sharing of user data are required to go through an internal design review process. Google has also established incident response processes to report and handle events related to confidentiality. Google establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchange with external parties.

## **Network Architecture and Management**

The Google Cloud Platform system architecture utilizes a fully redundant network infrastructure. Google has implemented perimeter devices to protect the Google network from external attacks. Network monitoring mechanisms are in place to prevent access to the Google network from unauthorized devices.

## **People**

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform products to customers. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes; the hiring and development of highly skilled resources; and leading industry practices. Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, and confidentiality controls.

Formal organizational structures exist and are available to Google employees on the Company's intranet. The intranet provides drill-down functionality for identifying employees in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to

segregate duties and enforce responsibilities based on job functionality. Policies and procedures are reviewed and updated as necessary.

## **Attachment B - Principal Service Commitments and System Requirements**

### **Service Commitments**

Commitments are declarations made by management to customers regarding the performance of Google Cloud Platform. Commitments to customers are communicated via Terms of Service, Google Cloud Platform Service Level Agreements, and Data Processing Addendums.

### **System Requirements**

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform System products to customers. These internal policies are developed in consideration of legal and regulatory obligations, to define Google's organizational approach and system requirements.

The delivery of these services depends upon the appropriate internal functioning of system requirements defined by Google to meet customer commitments.

The following processes and system requirements function to meet Google's commitments to customers with respect to the terms governing the processing and security of customer data:

- **Access Security:** Google maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege.
- **Change Management:** Google requires standard change management procedures to be applied during the design, development, deployment, and maintenance of all Google Applications, Systems, and Services.
- **Incident Management:** Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.
- **Data Management:** Google complies with any obligations applicable to it with respect to the processing of Customer Personal Data. Google processes data in accordance with the customer instructions and complies with applicable regulations.
- **Data Security:** Google implements and maintains technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Google takes 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.
- **Third Party Risk Management:** Google conducts routine inspections of sub-processors to evaluate control conformance. Google defines the security and privacy obligations which the sub-processor must meet to satisfy Google's obligations regarding customer data, prior to Google granting access to customer data.