Google

System and Organization Controls (SOC) 3

Report over the Google Workspace, Application Programming Interfaces and Developer Offerings System

Relevant to Security, Availability, Confidentiality, and Privacy

For the Period 1 May 2022 to 30 April 2023

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Google Workspace, Application Programming Interfaces and Developer Offerings System
Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy

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

- Identifying the Google Workspace, Application Programming Interfaces and Developer Offerings System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our service commitments and system requirements
- Identifying the risks that would threaten the achievement of its 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 System to mitigate risks that threaten the achievement of the 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 May 2022 to 30 April 2023, to provide reasonable assurance that the service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy 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
14 June 2023

Report of Independent Accountants

To the Management of Google LLC:

Scope

We have examined management's assertion, contained within the accompanying report titled "Management's Report of its Assertions on the Effectiveness of Its Controls Over the Google Workspace, Application Programming Interfaces and Developer Offerings System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy" (Assertion), that Google's controls over the Google Workspace, Application Programming Interfaces and Developer Offerings System (System) were effective throughout the period 1 May 2022 to 30 April 2023, to provide reasonable assurance that its service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy (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's 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 Workspace, Application Programming Interfaces and Developer Offerings System (System) and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and system requirements that are the objectives of the System
- Identifying, designing, implementing, operating, and monitoring effective controls over the Google Workspace, Application Programming Interfaces and Developer Offerings System (System) to mitigate risks that threaten the achievement of the 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 ("AICPA"). 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, confidentiality, and privacy 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.

We are required to be independent of Google and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Control Standards.

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 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 May 2022 to 30 April 2023, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

14 June 2023
San Jose, CA

Attachment A - Google Workspace, Application Programming Interfaces and Developer Offerings System

Overview

Google LLC ("Google" or "the Company"), an Alphabet subsidiary, 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's product offerings, including Google Workspace, Application Programming Interfaces and Developer Offerings (Google Workspace Services), 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.

Google Workspace, Application Programming Interfaces and Developer Offerings are targeted to small and medium businesses and large corporations alike. These products provide what business organizations typically require, including the following:

- Multi-user collaboration
- No special hardware or software required by the enterprise
- Security and compliance features
- Seamless upgrades

The products are composed of communication, productivity, collaboration and security tools that can be accessed virtually from 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.

Google Workspace Editions / SKUs

The Google Workspace brand is reflected in the related agreements and supporting documentation made available by Google.

G Suite Basic

- "G Suite Basic" is an edition of Google Workspace composed of all of the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, Google Workspace Migrate, and Workspace Add-ons.

"Workspace Add-Ons" are, collectively, Google SIP Link, Google Voice, Google Workspace Assured Controls, Workspace Additional Storage, and Meet Global Dialing.

G Suite Business

- "G Suite Business" is an edition of Google Workspace composed of all of the Google Workspace Services except Client-Side Encryption and Workspace Add-Ons. G Suite Business also includes data region policy settings for primary data within Customer Data for certain Services.

Google Workspace Business Starter

- "Google Workspace Business Starter" is an edition of Google Workspace composed of all of the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, Google Workspace Migrate, and Workspace Add-Ons. Google Workspace Business Starter Customers are limited to a maximum of 300 End Users.

Google Workspace Business Standard

- "Google Workspace Business Standard" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, and Workspace Add-Ons. Google Workspace Business Standard Customers are limited to a maximum of 300 end users.

Google Workspace Business Plus

- "Google Workspace Business Plus" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Cloud Search, and Workspace Add-Ons. Google Workspace Business Plus Customers are limited to a maximum of 300 end users.

Google Workspace Enterprise Starter

- "Google Workspace Enterprise Starter" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, and Workspace Add-Ons.

Google Workspace Enterprise Standard

- "Google Workspace Enterprise Standard" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Cloud Search, and Workspace Add-Ons. Google Workspace Enterprise Standard also includes data loss prevention functionality for Gmail and Google Drive, and certain enhanced security and control features for administrators (not including Google Workspace Security Center). Google Workspace Enterprise Standard will also allow for additional Gmail integration with other Google products, certain third-party archiving tools, and third-party OAuth applications.

Google Workspace Enterprise Plus

- "Google Workspace Enterprise Plus" is an edition of Google Workspace composed of all the Google Workspace Services except Workspace Add-Ons. Google Workspace Enterprise Plus also includes data loss prevention functionality for Gmail and Google Drive, data region policy settings for primary data within customer data for certain services, additional search and assist capabilities for content within third-party data sources (which are only available to

customers with at least 500 End User licenses), and enhanced security and control features for administrators (including Google Workspace Security Center). Google Workspace Enterprise Plus will also allow for additional Gmail integration with other Google products, certain third-party archiving tools, and third-party OAuth applications.

Google Workspace for Education

- "Google Workspace for Education Fundamentals" is a free edition of Google Workspace composed of the Google Workspace Services except Client-Side Encryption, Currents, Google Cloud Search, Google Workspace Migrate, and Workspace Add-Ons. This edition also includes Assignments, Classroom and Chrome Sync as Core Services.
- "Google Workspace for Education Standard" is an upgrade to Google Workspace for Education Fundamentals that is available at an additional cost. It includes additional features such as data region policy settings for primary data within customer data for certain services, advanced security controls, enhanced analytics, and Google Workspace Migrate.
- "Google Workspace for Education Teaching and Learning Upgrade" is an upgrade to Google Workspace for Education Fundamentals that is available at an additional cost. It includes additional features for communication, collaboration, class management, and additional storage equal to 100GBs times the number of end user licenses.
- "Google Workspace for Education Plus" is an upgrade to Google Workspace for Education Fundamentals that is available at an additional cost. It includes additional features such as data region policy settings for primary data within customer data for certain services, advanced controls, enhanced analytics and search (but search and assist capabilities for content within third party data sources are only available to customers with at least 500 End User licenses), Google Workspace Migrate, and additional features for communication, collaboration, class management, and additional storage equal to 20GBs times the number of end user licenses.

Google Workspace Archived User

- The "Archived User" offering for each Google Workspace or G Suite edition allows an organization to maintain End User Accounts for former End Users for Customer's data archival purposes. The following editions of Google Workspace Archived User include Google Vault:

  - G Suite Business - Archived User
  - Google Workspace Business Plus - Archived User
  - Google Workspace Enterprise Standard - Archived User
  - Google Workspace Enterprise Plus - Archived User

Google Workspace Essentials Starter

- "Google Workspace Essentials Starter" is a free edition of Google Workspace comprised of the services within the "Google Workspace Essentials" edition, but with different storage capacities. Customers will have a limit of 100 total end users licenses.

Google Workspace Essentials

- "Google Workspace Essentials" is an edition of Google Workspace composed of Google Calendar, Google Chat, Google Docs, Google Drive, Google Forms, Google Jamboard, Google Keep, Google Meet, Google Sheets, Google Sites, Google Slides, and Google Tasks and the following as used in conjunction with the foregoing Services: (a) Cloud Identity Management, (b) Google Contacts, and (c) Google Groups for Business.

Google Workspace Enterprise Essentials

- "Google Workspace Enterprise Essentials" is an edition of Google Workspace composed of the services within the "Google Workspace Essentials" edition, but with different storage capabilities.

Google Workspace Enterprise Essentials Plus

- "Google Workspace Enterprise Essentials Plus" is an edition of Google Workspace composed of the services within the "Google Workspace Essentials" edition, but with the following features: (a) Google Workspace Enterprise Essentials Plus also includes data loss prevention functionality for Google Drive, data region policy settings for primary data within customer data for certain services, and certain enhanced security and control features for administrators (including Google Workspace Security Center); and (b) different storage capabilities.

Google Workspace Frontline

- "Google Workspace Frontline Starter" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, Google Workspace Migrate, and the Workspace Add-Ons.
- "Google Workspace Frontline Standard" is an edition of Google Workspace composed of all the Google Workspace Services except Google Cloud Search, Google Workspace Migrate, and the Workspace Add-Ons. Google Workspace Frontline Standard also includes data loss prevention functionality for Gmail and Google Drive, and certain enhanced security and control features for Administrators (not including Google Workspace Security Center).

Google Workspace for Nonprofits

- "Google Workspace for Nonprofits" is a free edition of Google Workspace composed of the Google Workspace Services except Client-Side Encryption, Currents, Google Cloud Search, Google Workspace Migrate, and the Workspace Add-Ons. This edition also includes Classroom (as defined in "Google Workspace for Education Fundamentals" above) as a Core Service.

Cloud Search Platform

- "Cloud Search Platform" is an edition of Google Workspace composed of Google Cloud Search and the following services for use in conjunction with Google Cloud Search: (a) Cloud Identity Management; (b) Google Contacts; and (c) Google Groups for Business. Cloud Search Platform provides search and assist capabilities for content within third-party data sources.

Google Workspace Add-ons

Google Voice and Google SIP Link

- "Voice Starter" is a version of Google Voice that can be added at an additional cost to any edition of Google Workspace and that allows only up to 10 end users in a single country.
- "Voice Standard" is a version of Google Voice that can be added at an additional cost to any edition of Google Workspace and that supports any number of end users in a single country. Voice Standard also includes Google SIP Link, deskphone compatibility, and multi-level auto-attendant features.
- "Voice Premier" is a version of Google Voice that can be added at an additional cost to any edition of Google Workspace that supports any number of end users in multiple countries. Voice Premier also includes Google SIP Link, deskphone compatibility, multi-level auto-attendant features, and advanced reporting functionality.
- "Google SIP Link Standard" is a version of Google SIP Link that can be added at an additional cost to any edition of Google Workspace and that supports any number of end users in a single country. Google SIP Link Standard also includes deskphone compatibility and multi-level auto-attendant features.
- "Google SIP Link Premier" is a version of Google SIP Link that can be added at an additional cost to any edition of Google Workspace and that supports any number of end users in multiple countries. Google SIP Link Premier also includes deskphone compatibility, multi-level auto-attendant features, and advanced reporting functionality.

Google Workspace Assured Controls

- "Google Workspace Assured Controls" is a separate SKU that can be added at an additional cost to the Google Workspace Enterprise Plus edition. Google Workspace Assured Controls allows customers to geographically limit Google support actions related to their customer data.

Meet Global Dialing

- "Meet Global Dialing" is a separate SKU that can be added to any Google Workspace edition and that supports expanded dial-in and dial-out calling in Google Meet video meetings. There is no cost to subscribe to Meet Global Dialing, but usage is charged per minute.

Workspace Additional Storage

- "Workspace Additional Storage" is a separate SKU that can be added at an additional cost to any edition of Google Workspace as long as that edition does not limit storage on a per-End User basis. Customers may increase their total amount of pooled storage available by 10TB for each Workspace Additional Storage subscription purchased. There is no limit to the number of Workspace Additional Storage subscriptions that may be purchased.

The Google Workspace, Application Programming Interfaces and Developer Offerings (Google Workspace Services) covered in this system description consist of the following:

Google Workspace Core Services

Google Workspace Core Services are a set of applications, including Gmail, Docs, Sheets, Slides, Sites, and more, as well as a set of messaging, collaboration and security tools for organizations.

Admin Console

Google Admin Console is a management tool for Google Workspace administrators. It allows administrators to maintain all their Google Workspace services from one console. With the Google Admin Console, administrators can configure settings for Google Workspace, monitor the usage of their domains, and create user accounts.

Assignments

Assignments is an application for learning management systems that allows customer end users to distribute, collect, and grade student work.

Classroom

Classroom is a web-based service that allows customer end users to create and participate in classroom groups. Using Classroom, students can view assignments, submit homework, and receive grades from teachers.

Cloud Identity

Cloud Identity is an Identity as a Service (IDaaS) and enterprise mobility management (EMM) product. It offers the identity services and endpoint administration that are available in Google Workspace as a stand-alone product.

Cloud Search

Cloud Search is a web-based service that provides customer end users with search and assist capabilities for content within certain Google Workspace Core Services and selected third-party data sources. Google Cloud Search also provides end users with actionable information and recommendations.

Currents

Currents is a web-based service that allows customer end users to share links, videos, pictures, and other content with others within the same Google Workspace domain, and to view and interact with content shared with them by others within that same domain. Customer end users can also create and join communities to have conversations with others within the same domain who share their interests.

Gmail

Gmail is a web-based e-mail service that allows an organization to run its e-mail system using Google's systems. It provides the capability to access an end user's inbox from a supported web browser, read mail, compose, reply to, and forward mail, search mail, and manage mail through labels. It provides filtering for spam and viruses and allows administrators to create rules for handling messages containing specific content and file attachments or routing messages to other mail servers.

Google Calendar

Calendar is a web-based service for managing personal, corporate/organizational, and team calendars. It provides an interface for customer end users to view their calendars, schedule meetings with other end users, see availability information of other end users, and schedule rooms and resources.

Google Chat

Chat is a web-based service that allows for real time communication between customer end users. The service provides an enhanced chat messaging and group collaboration platform that allows content integrations with select third-party services.

Google Contacts

Contacts is a web-based service that allows customer end users to import, store, and view contact information, and create personal groups of contacts that can be used to email many people at once.

Google Docs

Docs is a web-based service that enables customer end users to create, edit, share, collaborate, draw, export, and embed content on documents.

Google Drive

Drive provides web-based tools enabling customer end users to create, store, transfer, and share files, and view videos.

Google Forms

Forms is a web-based service that enables customer end users to create, edit, share, collaborate, export, and embed content in forms.

Google Groups for Business

Groups is a web-based service that allows customer end users and website owners to create and manage collaborative groups to facilitate discussions and content sharing.

Google Hangouts*

Hangouts is a web-based service that allows for real time communication between customer end users. The service provides one-on-one and group conversations via chat messaging, and voice, as well as lightweight video meetings.

Google Jamboard

Jamboard is a web-based service that allows customer end users to create, edit, share, collaborate, draw, export, and embed content within a document.

Google Keep

Keep is a web-based service that enables customer end users to create, edit, share, and collaborate on notes, lists, and drawings.

Google Meet

Meet is a web-based service that allows for real time communication between customer end users. The service provides enhanced large-capacity video meetings.

Google Sheets

Sheets is a web-based service that enables customer end users to create, edit, share, collaborate, draw, export, and embed content on spreadsheets.

Google Sites

Sites allows end users to create a site through a web-based tool, and then can share the site with a group of other end users or publish the site to the entire company or the world (if permitted by the Administrator). The site owner can choose who can edit a site and who can view the site.

Google Slides

Slides is a web-based service that enables customer end users to create, edit, share, collaborate, draw, export, and embed content on presentations.

Google Tasks

Tasks is a web-based service that enables customer end users to create, edit, and manage their tasks.

Google Vault

Vault is a web-based service that provides search and export capabilities for Google Drive and Gmail. For Gmail, Google Vault provides customers with the ability to search across the entire domain, to archive data, and create retention and disposition rules based on content, and eDiscovery capabilities which allow a customer to create matters and preserve this data for legal hold purposes.

Google Voice

Google Voice is an admin-managed Internet Protocol (IP)-based telephony service. It allows customers to assign and manage phone numbers for use by end users in their organization. End users can make and receive calls using their assigned numbers; additional functionalities are also available for use in connection with inbound and outbound calling, including the dialing of emergency numbers for end users using two-way dialing.

Google Workspace Migrate

Google Workspace Migrate provides data migration solutions that enable customers to easily move their on-premises or other-cloud data into Google Workspace.

Mobile Device Management

Organizations can use Google Mobile Device Management to manage, secure, and monitor mobile devices in their organization. Administrators can manage a range of devices, including phones, tablets, and smartwatches.

* Google Hangouts was deprecated on 1 November 2022

Application Programming Interfaces (APIs) and Developer Offerings

Application Programming Interfaces (APIs) and Developer Offerings are collection of tools and resources that let customers integrate their software with Google Workspace and its users or develop new apps that run entirely within Google Workspace. The offerings included in this system description are Apps Script, Product APIs and the Admin Software Development Kits (SDK).

Apps Script

Google Apps Script is a rapid application development platform that makes it fast and easy to create business applications that integrate with Google Workspace.

Product APIs

Product APIs allow applications to integrate with Google Workspace products and other Google Workspace data.

Calendar API

Calendar API enables the creation of new events in a user's Google Calendar, editing or deleting existing events, and searching for events.

Contacts API*

Contacts API allows client applications to view and update a user's contacts. Contacts are stored in the user's Google Account; most Google services have access to the contact list.

Drive Activity API

Drive Activity API lets a customer's application retrieve information about a user's Google Drive activity. This API provides additional functionality on top of the existing Drive API to display activity on a user's profile, track changes to specific files or folders, and alert a user to new comments or changes to file.

Drive Rest API

Drive Rest API allows applications to interact with nearly any aspect of a user's Google Drive, including permissions, file revisions, and connected apps.

Gmail Rest API

Gmail Rest API enables applications to read messages from Gmail, send emails, modify the labels applied to messages and threads, and search through existing mail.

People API

People API enables applications to read and manage the authenticated user's contacts, read and copy the authenticated user's "other contacts", read profile information for authenticated users and their contacts, and read domain profiles and contacts.

Sheets API

Sheets API provides comprehensive access to read, write, and format data in Google Sheets.

Sites API**

Sites Data API allows client applications to access and modify Google Site data using Google Data API feeds.

Tasks API

Tasks API provides access to search, read, and update organization-owned Google Tasks content and metadata.

Admin SDK

Admin SDK is a collection of tools which allows developers to write applications to manage Google Workspace domains, migrate from and integrate with existing IT infrastructure, create users, update settings, audit activity, and more. Scripts and add-ons (e.g., APIs) developed by end users are out of the scope of this report.

Alert Center API

Alert Center API lets customers manage alerts affecting their domain. Domain administrators can see and manage alerts manually from the Google Admin console. The Alert Center API lets apps customers retrieve alert data and alert feedback. The API can also create new alert feedback for existing alerts.

Data Transfer API

Data Transfer API manages the transfer of data from one user to another within a domain. One use case of this transfer is to reallocate application data belonging to a user who has left the organization.

Directory API

Directory API lets customers perform administrative operations on users, groups, organizational units, and devices in the organization's account.

Domain Shared Contacts API

Domain Shared Contacts API allows client applications to retrieve and update external contacts that are shared to all users in a Google Workspace domain.

Email Audit API

Google Workspace Email Audit API allows Google Workspace administrators to audit a user's email, email drafts, and archived chats. In addition, a domain administrator can download a user's mailbox.

Enterprise License Manager API

Enterprise License Manager API allows administrators to manage license assignments for Google Workspace services used by the organization.

Groups Migration API

Groups Migration API manages the migration of shared emails from public folders and distribution lists to a group's discussion archive.

Groups Settings API

Groups Settings API allows organizations to programmatically manipulate Google group settings for their domain.

Reports API

Reports API gives administrators of Google Workspace domains (including resellers) the ability to create custom usage reports for their domain.

Reseller API

Reseller API lets reseller administrators place customer orders and manage monthly postpaid subscriptions.

SAML-based SSO API

SAML-based SSO API enables customer end users to access their enterprise cloud applications by signing in one time for all services. If a user tries to sign-in to the Admin console or another Google service when SSO is set up, they are redirected to the SSO sign-in page.

* Contacts API was replaced by People API

** Sites API was deprecated on 30 January 2023

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 Workspace, Application Programming Interfaces and Developer Offerings:

North America, South America

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Clarksville (TN), United States of America
- Columbus (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Henderson (NV), United States of America
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America

- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Midlothian (TX), United States of America
- Moncks Corner (SC), United States of America
- Montreal, Quebec, Canada
- New Albany (OH), United States of America
- Osasco, Brazil
- Papillion (NE), United States of America
- Pryor Creek (OK), United States of America
- Quilicura, Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Toronto, Ontario, Canada
- Vinhedo, Brazil
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Doha (1), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- London (1), United Kingdom
- London (2), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain[+]
- Middenmeer, Netherlands
- Milan (1), Italy

- Milan (2), Italy
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Turin (1), Italy[+]
- Turin (2), Italy[+]
- Turin (3), Italy[+]
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland[+]
- Zurich, Switzerland

Asia Pacific

- Changhua, Taiwan
- Delhi (1), India
- Delhi (2), India[+]
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai, Chiba, Japan[+]
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Lok Yang Way, Singapore
- Loyang, Singapore[+]
- Melbourne, Victoria, Australia
- Mumbai (1), India
- Mumbai (2), India[+]
- Mumbai (3), India[+]
- Mumbai (4), India[+]
- Osaka, Japan
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea[+]
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia

- Wenya, Singapore

[+] Indicates data centers in scope only for the period 1 November 2022 through 30 April 2023

Infrastructure

Google Workspace, Application Programming Interfaces and Developer Offerings runs in a multi-tenant, distributed environment on synchronized internal system atomic clocks and global positioning systems (GPS). 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 Workspace, Application Programming Interfaces and Developer Offerings, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. User entity 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 its data centers for physical security to help protect production 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 monitoring mechanisms that provide 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 Workspace, Application Programming Interfaces and Developer Offerings 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. Google uses encryption to secure user data in transit between Google production facilities.

Google follows a formal process to grant or revoke employee, temporary worker, contractor or vendor 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. Additionally, access requests via "on demand request" mechanisms are reviewed and approved by a second individual prior to being granted and the event is logged.

Both user and internal access to customer data is restricted through the use of unique user account IDs and via the Google Accounts Bring Your Own Identity (BYOID) system externally. 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 code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented appropriately. Changes are developed and deployed utilizing source code management systems and release workflow automation tools to manage source code and document changes, facilitate releases, and perform other functions. Google requires all production-impacting 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 the production environment. Reviewed and submitted changes can be built into binaries. During the build process, code is subject to testing, the results of which are monitored by engineers during the creation of a candidate, which can then be deployed to QA or staging environments prior to deployment to production through a release. Changes to customer facing services that may affect confidentiality, processing integrity, and/or availability are communicated to relevant personnel and impacted customers.

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 Google personnel, including employees, temporary workers, vendors and contractors are required to complete these training programs at the time of joining the organization and annually thereafter. All new products and product feature launches that include collection, processing, or sharing of user data are required to go through an internal design review process that defines retention and deletion timelines. This review is performed by legal and privacy teams. In addition to the preventative controls, Google has also established detective measures to investigate and determine the validity of security threats. In the case of an incident there are incident response processes to report and handle events related to topics such as security, availability, and confidentiality. Google establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchange with external parties.

Network Architecture and Management

The Google Workspace, Application Programming Interfaces and Developer Offerings system architecture utilizes a fully redundant network infrastructure. Border routers that provide the connection point between Google Workspace, Application Programming Interfaces and Developer Offerings and any Internet Service Providers are designed to run in a redundant configuration. Where border routers are in use, firewalls are also implemented to operate in a redundant configuration. Google has implemented perimeter devices to protect the Google network from external attacks. Network monitoring mechanisms are in place to prevent and disconnect access to the Google network from unauthorized devices.

People

Google has implemented a process-based service quality environment designed to deliver the Google Workspace, Application Programming Interfaces and Developer Offerings 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, confidentiality, and privacy controls.

Google has established company structures and reporting lines and has helped ensure sufficient authorities are available to support compliance activities with regulatory, legal, contractual, and privacy requirements. Formal organizational structures exist and are available to Google personnel on the Company's intranet. The intranet provides drill-down functionality for identifying personnel 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 are reviewed annually, and other materials derived from policies, like guidelines, FAQs, and other related documents are reviewed and updated as needed.

Attachment B - Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Google Workspace, Application Programming Interfaces and Developer Offerings System. Commitments to customers are communicated via Terms of Service, Google Workspace, Application Programming Interfaces and Developer Offerings Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

Google has implemented a process-based service quality environment designed to deliver the Google Workspace, Application Programming Interfaces and Developer Offerings 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 security and privacy 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 Google applications, systems, and services
- **Incident Management:** Google monitors security event logs and alerts to determine the validity of security and privacy threats. Potential threats, including threats related to security and privacy, are escalated to the appropriate team including incident management. Google's dedicated security personnel will promptly investigate and respond to potential and 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 Google Workspace, Application Programming Interfaces and Developer Offerings Terms of Service and/or Data Processing Agreements, and complies with applicable regulations
- **Data Security:** Google maintains data security and privacy policies and implements 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 vendors to the extent applicable to their scope of performance

- **Third-Party Risk Management:** Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google conducts routine inspections of subprocessors to ensure their continued compliance with the agreed upon security and privacy requirements. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices