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 November 2023 to 31 October 2024

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 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) 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 our 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 and associated criteria that are the basis of our assertion

Complementary user entity controls: The Description also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Google's controls to achieve the service commitments and system requirements. The Description presents Google's controls and the complementary user entity controls assumed in the design of Google's controls.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period 1 November 2023 to 31 October 2024, to provide reasonable assurance that the service commitments and system requirements were achieved, if the complementary user entity controls assumed in the design of Google's controls operated effectively based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Google LLC
19 December 2024

Building a better
working world

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Service Auditor’s Report

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 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 November 2023 to 31 October 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria.*

Complementary user entity controls: The Description indicates that Google’s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Google’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Management's Responsibilities

Google’s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Google’s service commitments and system requirements were achieved. Google's management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, 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 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 service requirements that are the objectives of the System.

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 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 consider 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.

Our examination was also not conducted for the purpose of evaluating the performance or integrity of Google's AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Google's AI services.

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 November 2023 to 31 October 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary user entity controls assumed in the design of Google's controls operated effectively throughout that period.

Ernst + Young LLP

19 December 2024
San Jose, CA

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

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.

This report only applies to the infrastructure and underlying systems that support the Google Workspace products outlined below. The examination was also not conducted for the purpose of evaluating the performance or integrity of Google’s AI services or models.

Google Workspace Editions / SKUs

Google Workspace editions are combinations of Google Workspace Services for subscription purposes. Please refer to the Google Workspace Services Summary (https://workspace.google.com/terms/user_features/) for the Google Workspace Services that are included in each edition. Google Workspace Services are offered under the following editions:

- Google Workspace Business
- Google Workspace Enterprise
- Google Workspace Essentials
- Google Workspace Frontline
- Google Workspace for Education
- Google Workspace for Nonprofits
- G Suite (Legacy Version)

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.

Gemini for Google Workspace

Gemini for Google Workspace (formerly known as Duet AI for Google Workspace) allows customer end users to use generative artificial intelligence features to help write content, organize files, visualize information, accelerate workflows, and have richer meetings.

Gemini

Gemini is a conversational artificial intelligence assistant that enables customer end users to brainstorm ideas, spark creativity, and accelerate productivity. Gemini is included as a core service with these Gemini for Google Workspace add-ons: Gemini Enterprise, Gemini Business, Gemini Education and Gemini Education Premium. Gemini is in scope only for the period 1 August 2024 through 31 October 2024.

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 a customer 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 Drive for desktop is not in scope for this report.

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

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 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 customer 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 Vids

Google Vids is an AI-powered video-creation app for work. Vids lets customer end users create custom videos right in their web browser with no special software or video editing skills required. Google Vids is in scope only for the period 1 August 2024 through 31 October 2024.

Google Voice

Google Voice is an admin-managed Internet Protocol (IP)-based telephony service. It allows customer end users to assign and manage phone numbers for use by end users in their organization. Customer 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.

Read Along

Students can use Read Along to build reading skills on a computer or Android device. An in-app reading buddy uses Google's advanced text-to-speech and voice recognition technologies to listen and respond to students with real-time feedback and encouragement as they read aloud.

Application Programming Interfaces (APIs) and Developer Offerings

Application Programming Interfaces (APIs) and Developer Offerings are collections 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.

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.

Google Calendar API

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

Google Drive Activity API

Google 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.

Google Drive Rest API

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

Google Sheets API

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

Google Tasks API

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

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.

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 app 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.

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
- Chandler (AZ), United States of America**
- Clarksville (TN), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Gainesville (VA), United States of America
- Henderson (NV), United States of America
- Lancaster (OH), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America**
- Moncks Corner (SC), United States of America
- New Albany (OH), United States of America
- Omaha (NE), United States of America*
- Papillion (NE), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Reno (NV), United States of America
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Dublin, Ireland
- Eemshaven, Groningen, The Netherlands
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Middenmeer, Noord-Holland, The Netherlands

Asia Pacific

- Changhua, Taiwan
- Inzai City, Chiba, Japan
- Lok Yang Way, Singapore
- Wenya, Singapore

* Indicates data center is in scope only for the period 1 March 2024 through 31 October 2024

** Indicates data center is in scope only for the period 1 August 2024 through 31 October 2024

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. 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 its data centers and 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) and Secure Sockets Layer (SSL) 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. Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for Google Workspace, Application Programming Interfaces and Developer Offerings products is controlled via Access Control Lists (ACLs) thus limiting the use of these tools to only those individuals that have been specifically authorized.

Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to the Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication.

Google follows a formal process to grant or revoke personnel access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system which utilizes Secure Shell (SSH) and TLS/SSL certificates help provide secure and flexible access.

These mechanisms are designed to grant access rights to systems and data only to authorized users. Additionally, access requests via "on demand" mechanisms are reviewed and approved by an authorized 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 for external users. 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, and any inappropriate access identified is removed.

Access authorization in Google Workspace, Application Programming Interfaces and Developer Offerings products is enforced at all relevant layers of the system. The granting or modification of access rights is based on the user’s job responsibilities or on a need-to-know basis and must be authorized and approved by the user’s functional manager or system owners. Approvals are managed by workflow tools and are logged. Production system access is only granted to individuals who require this level of access to perform necessary tasks. Additionally, all users with access to production systems are required to complete security and privacy training annually. Access to individual production systems via critical access groups is reviewed on a periodic basis by the system owners and inappropriate access is removed for Google personnel who no longer have a business need for such access. Access to all corporate and production resources is automatically removed upon submission of a termination request by the manager of any departing employee, temporary worker, contractor or vendor, or by the appropriate Human Resources manager.

Change Management

Changes to Google Workspace, Application Programming Interfaces and Developer Offerings are delivered as software releases through three (3) pipelines:

- Product functionality change or builds related to the service running in Google's production environment;
- Images, downloads, or software updates made available to customers; and
- Open-source code packages maintained in a public source code repository.

Changes including configuration changes, code modifications, and new code creation, follow this change management process. Change Management policies and guidelines, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented. Each service has documented release processes that specify the procedures to be used, including definition of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping. Development, testing, and build environments are separated from the production environment through the use of logical security controls.

The change process starts with a developer checking out a copy of source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review, the change can be submitted making it the new head version. Google requires that production code reviewers be independent of the developer assigned to the change and follows Google coding standards, in accordance with their policy. Production code reviews are systematically enforced. Emergency changes to production environments must have a valid justification, and are logged, monitored and reviewed.

If needed, once the code is submitted, it can be used to build packages or binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built packages or binaries can be migrated to staging or QA environments where they can be subject to additional review. When the approved change is ready for deployment to production, it is deployed in a controlled manner, with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes, however, access to modify code and approve changes is controlled via functionality of internal tools that support the build and release process. Changes to customer facing services that may affect confidentiality, security, privacy, and/or availability are communicated to relevant personnel and impacted customers.

Guidelines are made available internally to govern the installation of software on organization-owned assets. Additionally, tools are utilized to detect deviations from pre-defined Operating System (OS) configurations on production machines and correct them automatically. This allows for an easy roll out of updates to system files in a consistent manner and helps ensure that machines remain in a known current state.

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. Relevant 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 network attacks and configurations of perimeter devices are centrally managed. Google segregates networks based on the types of services, users, and information systems. The network is managed via specialized tools. Google employs automated tools to inventory network devices and machines. Authorized security and network engineers access the network devices (production routers and switches) to monitor, maintain, manage, and secure the network through these tools.

Network monitoring mechanisms are in place to detect and prevent access to the Google network from unauthorized devices. Current and previous versions of each router configuration are maintained. Google has documented procedures and checklists for configuring and installing new servers, routers and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet.

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are permitted access to the network. The firewalls are designed to automatically deny all unauthorized packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the Secure Shell (SSH) protocol and two-factor authentication. Changes to network configurations are peer reviewed and approved prior to deployment. Google has implemented automated controls on network devices to identify distributed denial of service (DDOS) attacks. Google has established incident response processes to report and handle such events (see the Incident Management section).

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, including employees, temporary workers, vendors, and contractors, 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, frequently asked questions (FAQs), and other related documents are reviewed and updated as needed.

Complementary User Entity Control Considerations

Google Workspace, Application Programming Interfaces and Developer Offerings is designed with the assumption that user entities (also referred to as customers) would implement certain policies, procedures, and controls. In certain situations, the application of specific or additional controls at the user entity may be necessary to achieve the applicable trust criteria stated in the description.

This section describes those additional policies, procedures, and controls that Google recommends user entities should consider to complement Google's policies, procedures, and controls. Management of the user entity and the user entity's auditor should consider whether the following controls have been placed in operation at the user entity:

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Customers are responsible for providing the appropriate training to end-users on proper use of the Google Workspace, Application Programming Interfaces and Developer Offerings System consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use Policies available at (or such URL as Google may provide): • Google Workspace: https://workspace.google.com/terms/use_policy.html
	Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to the use of the Google Workspace, Application Programming Interfaces and Developer Offerings System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
	Customers should train administrators and end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Workspace, Application Programming Interfaces and Developer Offerings System.
Common Criteria 1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. Common Criteria 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
Common Criteria 2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. Common Criteria 2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Customers are responsible for defining, documenting, and making available to users procedures for the operation of their instance of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for identifying and managing the inventory of information assets on the Google Workspace, Application Programming Interfaces and Developer Offerings System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control. Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Customers should contact Google if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, and security events.
Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether	Customers are responsible for ensuring any application software which they deploy onto the Google Workspace, Application Programming Interfaces and Developer Offerings System follows their specific software change management policies and procedures.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
the components of internal control are present and functioning. Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Customers are responsible for periodically reviewing the configuration of the Google Workspace, Application Programming Interfaces and Developer Offerings System to ensure it is consistent with their policies and procedures.
Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Customers are responsible for establishing organizational policies and procedures for the use or integration of third-party services.
	Customers are responsible for reviewing the information security policies and the security capabilities in the Google Workspace, Application Programming Interfaces and Developer Offerings System to determine their applicability and modify their internal controls as appropriate.
	Customers are responsible for defining and maintaining policies and procedures governing the customer's administration of access to the Google Workspace, Application Programming Interfaces and Developer Offerings System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. Privacy Criteria 6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. Privacy Criteria 6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	Customers are responsible for establishing documented policies and procedures for the transfer and sharing of information within their organization and with third-party entities.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. Privacy Criteria 5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	Customers are responsible for provisioning, maintaining, monitoring and disabling end users' access in accordance with their internal access management policies.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Google Workspace, Application Programming Interfaces and Developer Offerings System consistent with customer organizational policies.
	Customers are responsible for implementing secure log-on procedures to access the Google Workspace, Application Programming Interfaces and Developer Offerings System consistent with customer access management policies.
	Customers are responsible for provisioning, maintaining, and disabling users' access in accordance with customer access management policies.
	Customers are responsible for reviewing users' access rights periodically, consistent with customer organizational policies, to mitigate the risk of inappropriate access.
	Customers are responsible for enabling and enforcing the use of two-step verification on privileged administrator accounts.
	Customers are responsible for establishing procedures to allocate the initial password to access the Google Workspace, Application Programming Interfaces and Developer Offerings System to end-users when Google password authentication is used.
	Customers are responsible for configuring third party Marketplace apps permissions in the Google Workspace Services consistent with their policies. Google Workspace Marketplace offers enterprise applications that can be added to a Google Workspace domain to enhance functionality and features to native Google applications.
	Customers are responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Google Workspace, Application Programming Interfaces and Developer Offerings System.

Trust Services Criteria	**Complementary User Entity Controls (CUECs)**
	Customers are responsible for configuring domain settings related to integration with other systems within the customer's environment consistent with customer policies.
	Customers are responsible for ensuring that user data is exported and deleted from the Google Workspace, Application Programming Interfaces and Developer Offerings System before or within a reasonable amount of time after termination.
Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Customers are responsible for ensuring appropriate physical security controls over all devices that access the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for ensuring any devices that access the Google Workspace, Application Programming Interfaces and Developer Offerings System or contain customer data are properly handled, secured, and transported as defined by the products requirements.
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Customers are responsible for configuring the Google Workspace, Application Programming Interfaces and Developer Offerings System mobile device options consistent with customer policies and procedures.

Trust Services Criteria	**Complementary User Entity Controls (CUECs)**
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Customers are responsible for enabling logging and monitoring functionalities to detect administrator activity, customer support activity, security events, system errors, and data deletions to support customer incident management processes.
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Workspace, Application Programming Interfaces and Developer Offerings System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.
	Customers are responsible for reviewing and testing features, builds, and product releases, including Application Programming Interfaces (APIs), to evaluate their impact prior to deploying into production environments, as applicable.
	Customers are responsible for configuring test and/or development environments in their instance of the Google Workspace, Application Programming Interfaces and Developer Offerings System, as applicable, and restricting access to data in these environments.
Common Criteria 9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Common Criteria 9.2: The entity assesses and manages risks associated with vendors and business partners.	Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google managed information systems that access the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for developing and maintaining disaster recovery and business continuity plans for their non-Google managed business systems.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality. Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity’s objectives related to privacy. Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity’s objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity’s objectives related to privacy.	Customers are responsible for ensuring that administrators do not send unnecessary employee personal data when escalating support requests to service providers, including Google.

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 or 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 help 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 help 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 help 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