



---

**System and Organization Controls (SOC) 3**  
**Report on the G Suite, Application Programming Interfaces and**  
**Developer Offerings System**  
**Relevant to Security, Availability, and Confidentiality**  
**For the Period 1 May 2019 to 30 April 2020**

---



Google LLC  
1600 Amphitheatre  
Parkway  
Mountain View, CA, 94043

650 253-0000 main  
Google.com

## **Management's Report on Its Assertions on the Effectiveness of Its Controls Over the G Suite, Application Programming Interfaces and Developer Offerings System**

### **Based on the Trust Services Criteria for Security, Availability, and Confidentiality**

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

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

We assert that the controls over the system were effective throughout the period 1 May 2019 to 30 April 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

**Google LLC**

15 June 2020



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 Accountants

To the Management of Google LLC:

### *Scope*

We have examined management's assertion, contained within the accompanying "Management's Report on Its Assertions on the Effectiveness of Its Controls over the G Suite, Application Programming Interfaces and Developer Offerings System Based on the Trust Services Criteria for Security, Availability and Confidentiality" (Assertion), that Google's controls over the G Suite, Application Programming Interfaces and Developer Offerings System (System) were effective throughout the period 1 May 2019 to 30 April 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

### *Management'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 G Suite, Application Programming Interfaces and Developer Offerings System (System) and describing the boundaries of the System
- Identifying its principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of its system
- Identifying, designing, implementing, operating, and monitoring effective controls over the G Suite, Application Programming Interfaces and Developer Offerings System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements

### *Our Responsibilities*

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (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, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other



procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

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

*Inherent limitations*

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

*Opinion*

In our opinion, Google's controls over the system were effective throughout the period 1 May 2019 to 30 April 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

*Ernst & Young LLP*

15 June 2020  
San Jose, CA

## Attachment A - G Suite, Application Programming Interfaces and Developer Offerings System

### G Suite, Application Programming Interfaces and Developer Offerings

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

Google’s product offerings, including G Suite, Application Programming Interfaces and Developer Offerings (G Suite 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.

G Suite, 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 comprised 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.

### G Suite Editions / SKUs

See ‘**Mapping of G Suite Services to Editions/SKUs**’ section below for a mapping of G Suite Services to their respective Editions or SKUs

#### G Suite Basic

- "G Suite Basic" is an edition of G Suite comprised of the G Suite Services, excluding Google Vault, Google Voice, and Google Cloud Search, which are available at additional cost

#### G Suite Business

- "G Suite Business" is an edition of G Suite comprised of all the G Suite Services, excluding Google Voice, and data region policy settings for primary data within Customer Data for certain Services. Customers that have five (5) or more end users will receive unlimited Google

Drive storage. Customers that have four (4) or fewer end users will receive 1TB of Google Drive storage for each end user

#### G Suite Business (Team Managed)

- "G Suite Business (Team Managed)" is an edition of G Suite offered under the G Suite Team Managed Agreement (prior version: Google Apps for Work Team Managed Agreement) which is comprised of Google Drive, Google Hangouts, Google Contacts, and Google+. Other G Suite Core Services are not available for team-managed accounts. Customers that have five (5) or more end users will receive unlimited Google Drive storage. Customers that have four (4) or fewer end users will receive 1TB of Google Drive storage for each end user

#### G Suite Enterprise

- "G Suite Enterprise" is an edition of G Suite comprised of all the G Suite Services excluding Google Voice. G Suite Enterprise 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, and enhanced security and control features for Administrators. G Suite Enterprise will also allow for additional Gmail integration with other Google products, certain third-party archiving tools, and third-party OAuth applications. Customers that have five (5) or more end users will receive unlimited Google Drive storage. Customers that have four (4) or fewer end users will receive 1TB of Google Drive storage for each end user

#### G Suite for Education

- "G Suite for Education" is a free edition of G Suite comprised of the G Suite Services, excluding Google+, Google Voice, and Google Cloud Search, and including Classroom and Chrome Sync. Customers that have five (5) or more end users will receive unlimited Google Drive storage. Customers that have four (4) or fewer end users will receive 1TB of Google Drive storage for each end user
- "G Suite Enterprise for Education" is a paid edition of G Suite comprised of services within the G Suite for Education edition and includes additional features such as data region policy settings for primary data within Customer Data for certain Services, advanced controls, enhanced analytics and search, and enterprise-grade communication tools

#### Drive Enterprise

- "Drive Enterprise" is an edition of G Suite comprised of Google Drive (including data loss prevention functionality) and the following as used in conjunction with Google Drive: (a) Cloud Identity Management; (b) Google Contacts; (c) Google Docs, Google Sheets, Google Slides and Google Forms; (d) Google Groups for Business; (e) Google Keep; (f) Google Sites; (g) Google Vault; (h) data region policy settings for primary data within Customer Data for certain Services; and (i) certain enhanced security and control features, migration tools, and mobile device management functionality for administrators

#### Cloud Search Platform

- "Cloud Search Platform" is an edition of G Suite comprised 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 Voice

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

### G Suite Archived User

- "G Suite Business - Archived User" is an edition of G Suite comprised of G Suite Services that allow an organization to maintain end user Accounts for former or inactive end users for Customer's data retention purposes and includes Google Vault. Customers will receive 1TB of Google Drive storage for each Archived End User Account
- "G Suite Enterprise - Archived User" is an edition of G Suite comprised of services within the G Suite Business - Archived User edition and includes additional data loss prevention functionality for Google Drive

The G Suite, Application Programming Interfaces and Developer Offerings covered in this system description consist of the following:

### **G Suite Core Services**

*G Suite 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 Google for G Suite administrators. It allows administrators to maintain all their G Suite services from one console. With the Google Admin Console, administrators can configure settings for G Suite, monitor the usage of their domains, and create user accounts.

### 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.

### 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 G Suite 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 G Suite Core Services and selected third-party data sources. Google Cloud Search also provides end users with actionable information and recommendations.

### 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.

### Docs

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

### Drive

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

### Forms

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

### 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+

Google+ is a web-based service that allows customer end users to share links, videos, pictures, collections, and other content with others within the same G Suite domain, and to view and interact with content shared with them by others within that same domain.

### 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 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 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.

## 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.

## 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.

## Keep

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

## 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.

## Sheets

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

## Sites (Classic/New)

Sites allows a customer end user to create websites on the G Suite Basic domain to publish internally within a company or publish externally. An end user can 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.

## Slides

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

## Talk\*\*

Google Talk is an instant messaging service that provides both text and voice communication. Google Talk is a legacy offering available to a select set of customers.

## Tasks

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

## 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.

## 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.

*\* Hangouts Chat and Hangouts Meet were rebranded as Google Chat and Google Meet in April 2020*

*\*\* product in scope for the period May 1, 2019 to October 31, 2019*

## **Application Programming Interfaces (APIs) and Developer Offerings**

*A collection of tools and resources that let customers integrate their software with G Suite and its users or develop new apps that run entirely within G Suite. 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 G Suite.

### Product APIs

Product APIs allow applications to integrate with G Suite products and other G Suite 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*

The Google Drive Activity API lets a customer's app retrieve information about a user's Google Drive activity. This API provides additional functionality on top of the existing Drive API.

### *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.

### *Email Settings API*

The Email Settings API enables administrators to programmatically manipulate most user-level Google Mail settings.

### *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.

### *Sheets API*

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

### *Sites API*

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

### *Tasks API*

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

### Admin SDK

Admin SDK is a collection of tools which allows developers to write applications to manage G Suite 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*

The 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 build retrieve alert data and alert feedback. The API can also create new alert feedback for existing alerts.

### *Apps Email Audit API*

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

### *Data Transfer API*

The 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*

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

### *Domain Shared Contacts API*

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

### *Enterprise License Manager API*

The Enterprise License Manager API allows administrators to manage license assignments for G Suite services used by the organization.

### *Groups Migration API*

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

### *Groups Settings API*

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

### *Reports API*

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

### *Reseller API*

The Reseller API lets reseller administrators place customer orders and manage monthly post-pay 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.

## Mapping of G Suite Services to Editions/SKUs

Product	Core Services	Basic	Business	Business (Team Managed)	Enterprise	Education	Cloud Identity	Drive Enterprise
Admin Console	✓	✓	✓		✓	✓	✓	✓
Calendar	✓	✓	✓		✓	✓		
Classroom						✓		
Cloud Identity	✓						✓	
Cloud Search	✓		✓		✓			
Contacts	✓	✓	✓	✓	✓	✓	✓	✓
Docs	✓	✓	✓	✓	✓	✓		✓
Drive	✓	✓	✓	✓	✓	✓		✓
Forms	✓	✓	✓	✓	✓	✓		✓
Gmail	✓	✓	✓		✓	✓		
Google+	✓	✓	✓	✓	✓			✓
Google Chat	✓	✓	✓	✓	✓	✓		
Google Hangouts	✓	✓	✓	✓	✓	✓		
Google Meet	✓	✓	✓	✓	✓	✓		
Groups	✓	✓	✓		✓	✓	✓	✓
Jamboard	✓	✓	✓		✓	✓		
Keep	✓	✓	✓		✓	✓		
Mobile Device Management	✓	✓	✓		✓		✓	✓
Sheets	✓	✓	✓	✓	✓	✓		✓
Sites	✓	✓	✓		✓	✓		✓
Slides	✓	✓	✓	✓	✓	✓		✓
Talk	✓	✓	✓		✓	✓		
Tasks	✓	✓	✓		✓	✓		
Vault	✓		✓		✓	✓		✓
Voice	✓				✓			
Apps Script		✓	✓	✓	✓	✓		✓
G Suite Product APIs		✓	✓	✓	✓	✓		✓
G Suite Admin SDK		✓	✓	✓	✓	✓	✓	✓

## 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 G Suite, Application Programming Interfaces and Developer Offerings:

- 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
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Hong Kong, Hong Kong
- Koto-ku, Tokyo, Japan
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- London (1), United Kingdom
- London (2), United Kingdom
- Los Angeles (CA), United States of America
- Moncks Corner (SC), United States of America
- Montreal, Quebec, Canada
- Mumbai, India
- Osaka, Japan
- Osasco, Brazil
- Pryor Creek (OK), United States of America
- Quilicura, Santiago, Chile
- Salt Lake City (UT), United States of America
- Seoul, South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Vinhedo, Brazil
- Wenya, Singapore
- Widows Creek (AL), United States of America

- Zurich, Switzerland

## **Infrastructure**

G Suite, Application Programming Interfaces and Developer Offerings runs in a multi-tenant, distributed environment. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For G Suite, 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. Structured data is then stored in large distributed databases, built on top of this file system.

## **Data Centers and Redundancy**

Google maintains consistent policies and standards across all data centers for physical security and environmental safeguards 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 a dashboard that provides details such as resource footprint, central processing unit capacity and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

## **Authentication and Access**

Strong authentication and access controls are implemented to restrict access to G Suite, 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. Data traffic is encrypted between Google production facilities.

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

Both user and internal access to customer data is restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user account ID, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data (and other need-to-know 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 semi-annual basis under the direction of the group administrators to help ensure

that access has been removed for employees who no longer have a business need or such access.

In May 2019, as part of Google's operations, Google identified a case where a subset of unhashed passwords was stored in their secure encrypted infrastructure for the period of January 2019 to May 2019. Google remediated the issue in May 2019 and followed established internal processes to notify the affected user base. This issue and remediation were also included in the last G Suite report issued in December 2019, which covers the period from 1 November 2018 to 31 October 2019. Other security controls such as encryption, access control and audit logging were in place to mitigate risk of misuse and Google found no evidence of misuse of these passwords. For additional details, please refer to Google's blog post [here](#).

## **Change Management**

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

## **Data**

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

## **Network Architecture and Management**

The G Suite, Application Programming Interfaces and Developer Offerings system architecture utilizes a fully redundant network infrastructure. Google has implemented perimeter devices to protect the Google network from external attacks. Network monitoring mechanisms are in place to prevent access to the Google network from unauthorized devices.

## **People**

Google has implemented a process-based service quality environment designed to deliver the G Suite, 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, and confidentiality controls.

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

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

With regard to the effect of the COVID-19 pandemic, there were no significant changes to the G Suite, Application Programming Interfaces and Developer Offerings which resulted in the failure to meet Google's principal service commitments and system requirements.

### **Service Commitments**

Commitments are declarations made by management to customers regarding the performance of G Suite, Application Programming Interfaces and Developer Offerings. Commitments to customers are communicated via Terms of Service, G Suite, Application Programming Interfaces and Developer Offerings Service Level Agreements, and Data Processing Addenda.

### **System Requirements**

Google has implemented a process-based service quality environment designed to deliver the G Suite, 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 processing and security of customer data:

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