



---

**System and Organization Controls (SOC) 3  
Report on the Google Firebase System  
Relevant to Security, Availability, and Confidentiality  
For the Period 1 November 2017 to 31 October 2018**

---

**SECTION I - Management's Assertion Regarding the Effectiveness of  
Its Controls Over the Google Firebase System Based on the Trust  
Services Principles and Criteria for Security, Availability, and  
Confidentiality**



Google LLC  
1600 Amphitheatre  
Parkway  
Mountain View, CA, 94043

650 253-0000 main  
Google.com

## **Management's Assertion Regarding the Effectiveness of Its Controls Over the Google Firebase System Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality**

We, as management of, Google LLC ("Google" or "the Company") are responsible for designing, implementing and maintaining effective controls over the Google Firebase System (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period 1 November 2017 to 31 October 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability, and confidentiality (Control Criteria) set forth in the American Institute of Certified Public Accountants' TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period 1 November 2017 to 31 October 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Google's commitments and system requirements



- the System was available for operation and use, to achieve Google's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Google's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Google Firebase System identifies the aspects of the Google Firebase covered by our assertion.

Very truly yours,

**GOOGLE LLC**  
14 December 2018

## **SECTION II - Report of Independent Accountants**



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

Management of Google LLC:

### Approach

We have examined management's assertion that Google maintained effective controls to provide reasonable assurance that:

- the Google Firebase System was protected against unauthorized access, use, or modification to achieve Google's commitments and system requirements
- the Google Firebase System was available for operation and use to achieve Google's commitments and system requirements
- the Google Firebase System information is collected, used, disclosed, and retained to achieve Google's commitments and system requirements

during the period 1 November 2017 through 31 October 2018 based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Google's management. Our responsibility is to express an opinion based on our examination.

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its



commitments and system requirements related to security, availability, and confidentiality are achieved.

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. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### **Opinion**

In our opinion, Google's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

*Ernst & Young LLP*

14 December 2018  
San Jose, CA

## **SECTION III - Description of the Google Firebase System**



## Description of the Google Firebase System

### Google Overview

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 web site 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 web sites 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.

Firebase is a mobile app platform (platform as a service) offered by Google with an integrated, unified software development kit (SDK), hereafter described collectively as (Firebase). Firebase provides developers with a rich suite of tools and resources to develop and manage high quality apps, for growing their user base, and to monetize the platform. It consists of complementary features that work independently, or can be mix-and-matched as needed.

Leveraging Google's cloud environment, Firebase can be accessed from virtually any location with Internet connectivity. This means every developer and each user they work with can be productive from anywhere, using any device with an Internet connection.

The Firebase services covered in this system description consist of the following:

- Cloud Firestore
- Cloud Functions for Firebase
- Cloud Storage for Firebase
- Firebase A/B Testing
- Firebase Authentication
- Firebase Cloud Messaging
- Firebase Console
- Firebase Crash Reporting
- Firebase Dynamic Links
- Firebase Hosting
- Firebase In-App Messaging
- Firebase Invites
- Firebase Performance Monitoring
- Firebase Predictions
- Firebase Realtime Database
- Firebase Remote Config
- Firebase Test Lab
- Google Analytics for Firebase
- ML Kit for Firebase

### *Cloud Firestore*

Cloud Firestore is a flexible, scalable database for mobile, web, and server development from Firebase and Google Cloud Platform. Like Firebase Real-time Database, it keeps customer data in sync across client apps through realtime listeners and offers offline support for mobile and web so user entities can build responsive apps.

### *Cloud Functions for Firebase*

Cloud Functions for Firebase are developer tools that simplify the development and deployment of Google Cloud Functions, a service offered by Google Cloud Platform. Google Cloud Functions enable user entities to run their own backend code that executes automatically based on HTTP requests and Firebase and Google Cloud Platform events. With Google Cloud Functions there's no need for user entities to manage their own server. User entity functions are stored in Google's cloud and run in a managed Node.js environment.

### *Cloud Storage for Firebase*

Cloud Storage for Firebase is a RESTful service for storing and accessing data on Google's infrastructure. The service combines the performance and scalability of Google's cloud with advanced security and sharing capabilities.

### *Firebase A/B Testing*

Firebase A/B Testing allows developers to make data-driven decisions about the actions they might take on their apps. Developers can run controlled experiments with Firebase Remote Config parameters to compare alternative scenarios, and see which one performs better in reaching their goals.

### *Firebase Authentication*

Firebase Authentication is a fully managed user identity and authentication system providing backend services, easy-to-use SDKs and ready-made UI libraries enabling seamless sign-in and sign-up experiences for an application or service.

### *Firebase Cloud Messaging*

Firebase Cloud Messaging (FCM) is a cross-platform messaging solution that lets developers reliably deliver messages to devices. Using FCM, developers can notify a client app that new email or other data is available to sync. Developers can send notification messages to drive user re-engagement and retention.

### *Firebase Console*

Firebase Console is the web developer console and Firebase Services API that helps developers get started, configure, and use Firebase services. This includes offering insight into shared

services, administrative services, web applications, data analysis, virtual machines, datastore, databases, networking, and developer services.

### *Firebase Crash Reporting*

Crash Reporting creates detailed reports of the errors in an application. Errors are grouped into issues based on having similar stack traces, and triaged by the severity of impact on users. In addition to automatic reports, developers can log custom events to help capture the steps leading up to a crash.

### *Firebase Dynamic Links*

Firebase Dynamic Links are smart URLs that allow user entities to send existing and potential users to any location within their iOS, Android, or web application. Firebase Dynamic Links survive the application install process, so even new users will see the content they're looking for when they open the app for the first time.

### *Firebase Hosting*

Firebase Hosting is developer-focused static web hosting for modern front-end web applications. Using Firebase Hosting, developers can deploy SSL-enabled web apps to a global content-delivery network from a single command.

### *Firebase In-App Messaging*

In-app messaging enables an application to drive engagement by sending well-designed, targeted messages to its users, without any engineering effort, from the Firebase console.\*

### *Firebase Invites*

Firebase Invites makes it simple for users to send content to their friends, over both SMS and email, by ensuring that referral codes, recipe entries, or other shared content gets passed along with the invitation. Firebase Invites builds on Firebase Dynamic Links, which ensures that recipients of links have the best possible experience for their platform and the apps they have installed.

### *Firebase Performance Monitoring*

Firebase Performance Monitoring is a service that helps developers to gain insight into the performance characteristics of their iOS and Android apps. Developers use the Performance Monitoring SDK to collect performance data from their applications, and then review and analyze that data in the Firebase console. Performance Monitoring helps developers understand where and when the performance of their applications can be improved so that they can use that information to fix performance issues.

---

\* The Firebase In-App Messaging SDK are optional tools and are outside the scope of this attestation.

### *Firestore Predictions*

Firestore Predictions applies machine learning to a developer's analytics data to create dynamic user groups based on their users' predicted behavior. These predictions are automatically available for use with Firestore Remote Config, the Notifications composer, and A/B testing.

### *Firestore Realtime Database*

The Firestore Realtime Database is a cloud-hosted, NoSQL database. Data is stored as JSON and synchronized in realtime to every connected client. When a developer builds cross-platform apps with Google's iOS, Android, and JavaScript SDKs, all of their clients share one Realtime Database instance and automatically receive updates with the newest data.

### *Firestore Remote Config*

Firestore Remote Config allows developers to customize how their app renders for each user, change the app's look and feel, roll out features gradually, run A/B tests, deliver customized content to certain users, or make other updates without deploying a new version—all from the Firestore console.

### *Firestore Test Lab*

Firestore Test Lab for Android provides cloud-based infrastructure for testing apps on physical and virtual devices. With a single operation, developers can test their apps across a wide variety of devices.

### *Google Analytics for Firestore*

Google Analytics for Firestore is an application measurement solution that provides insight on app usage and user engagement.

### *ML Kit for Firestore*

ML Kit for Firestore makes the power of machine learning accessible to all mobile developers. The SDK seamlessly blends on-device and cloud APIs to give developers solutions to common yet important problems without requiring deep knowledge of machine learning, neural networks, or model optimization. More advanced ML practitioners are able to use this service to dynamically serve and update mobile-optimized custom models to their end users.

## **Infrastructure**

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



### *Data Centers and Redundancy*

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

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

Firebase Hosting and Firebase Realtime Database backups are periodically performed to support the availability of user entity data. Firebase Hosting and Firebase Realtime Database data restore tests are periodically performed to confirm the ability to recover customer data. Critical data is replicated to at least two (2) data centers and provides high availability by dynamically load balancing across those sites.

### *Authentication and Access*

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

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

Both user and internal access to customer data is restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user account ID, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semi-annual basis under the direction of the group administrators.

## *Change Management*

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

## **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 non-disclosure agreements, for preserving confidentiality of information and software exchange with external parties.

## **Network Architecture and Management**

The Google Firebase 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 and disconnect access to the Google network from unauthorized devices.

## **People**

Google has implemented a process-based service quality environment designed to deliver the Google Firebase 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.