Google Cloud whitepaper
November 2019

Trusting your data with G Suite

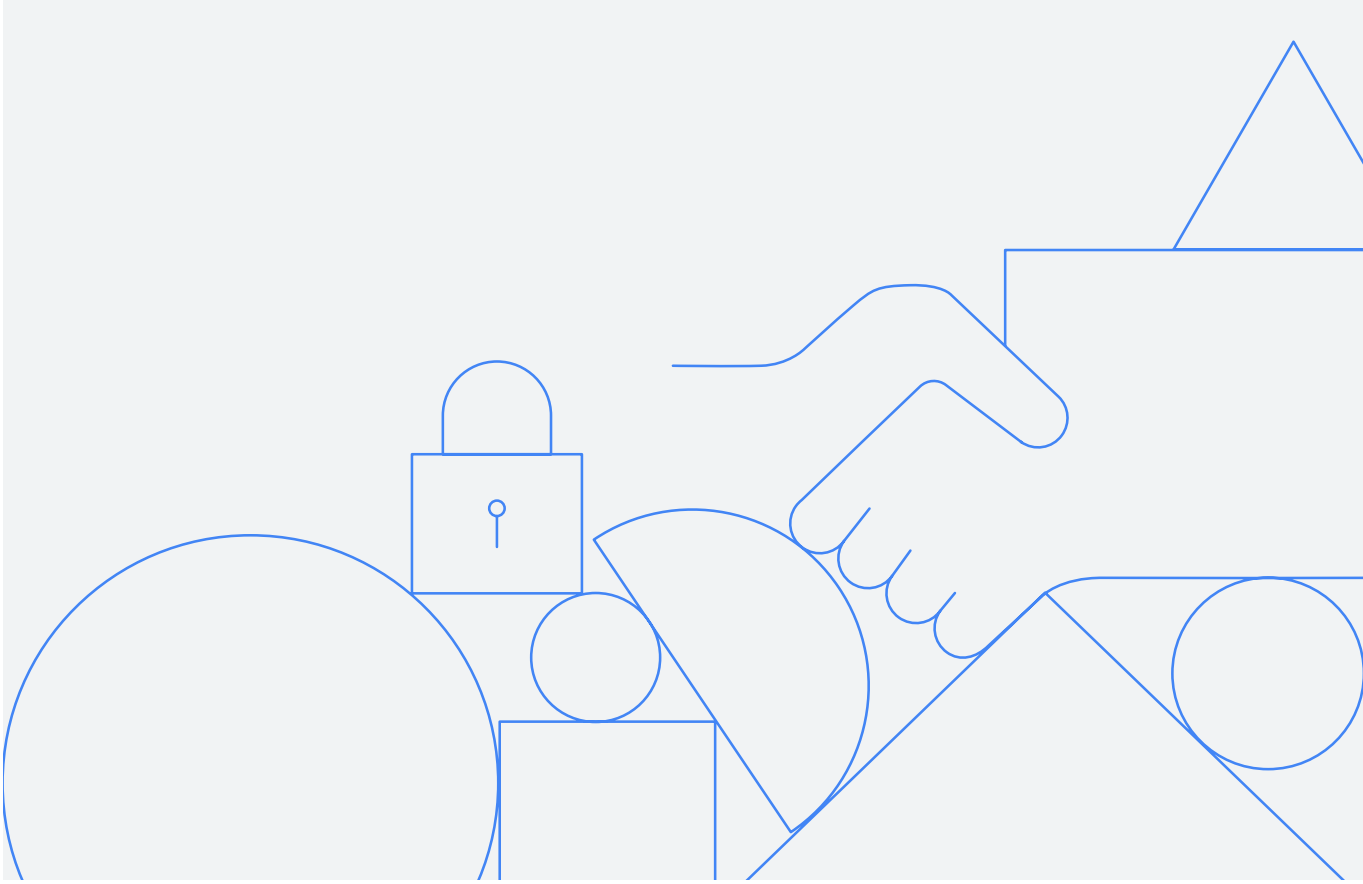


Table of contents

The information contained herein is intended to outline general product direction and should not be relied upon in making purchasing decisions nor shall it be used to trade in the securities of Alphabet Inc. The content is for informational purposes only and may not be incorporated into any contract. The information presented is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Any references to the development, release, and timing of any features or functionality described for these services remains at Google's sole discretion. Product capabilities, timeframes and features are subject to change and should not be viewed as Google commitments.

1. Introduction

At Google Cloud we've set a high bar for what it means to host, serve, and protect customer data. Security and data protection are at the core of how we design and build our products. We start from the fundamental premise that Google Cloud customers own their data and control how it is used. The data that a customer stores and manages in G Suite is only used to provide that customer with G Suite services. These services are provided in accordance with the customer's contract[1] and for no other purpose - not for advertising, not for anything else. Our Google Cloud Trust Principles[2] summarize our commitment to securing and protecting the privacy of data stored by customers in Google Cloud.

This whitepaper provides details about how we protect customer data throughout its lifecycle as well as how we provide customers with transparency and control over their data in G Suite. G Suite offers built-in data protection at scale, by default, designed to protect your business from intrusions, theft, and attacks. Customer data in G Suite is encrypted at rest[3] by default and, depending on the connection, Google applies default protections to customer data in transit.[4] In addition to continuous security monitoring for external threats, we explain the robust controls and auditing in place to protect against insider access to customer data. These include providing customers with near real-time logs of Google administrator access data, where available. If you'd like to learn more about how we define customer data, please refer to our G Suite Terms.[5]

G Suite products regularly undergo independent, third-party audits and certifications to verify that our data protection practices match our controls and commitments. An overview of our key compliance reports and certifications, as well as how we support our customers with their compliance journey, is also provided in this paper.

[1] Including additional instructions provided by the customer in accordance with the contract, for example, instructions provided to Google through the Admin console.
[2] Page 3, Privacy
[3] Page 3, How Google Uses Encryption to Protect Your Data
[4] Page 3, How Google Uses Encryption to Protect Your Data
[5] Page 3, G Suite (Online) Agreement

2. Managing your data lifecycle on G Suite

This section describes the data lifecycle in G Suite through the lens of security and privacy, including G Suite features that can help reduce common risks.

2.1 Data protection

Using G Suite services involves transferring data between your computer (typically via your browser) or mobile device, Google's servers and, sometimes, other users. Google enables encryption in transit[6] by default between your device and our data centers, and uses Transport Layer Security (TLS) protocol to encrypt requests before transmission outside Google. This helps prevent third parties from **exploiting vulnerabilities** in internet connections to access sensitive data.

To help protect your emails, chats, Google Drive files and other data in storage, G Suite customer data is **encrypted at rest** without the customer having to take any action. For further information on encryption, please see our G Suite Encryption whitepaper.[7]

Customers can **control access** to data and services on G Suite to help ensure that data is protected in accordance with the organization's desired configuration. **Role-based access controls** enable customers to appoint users as administrators,[8] granting the user the ability to access and perform certain tasks in the G Suite Admin console. You can make a user a super administrator who can perform all tasks in the Admin console. Or you can assign a role that limits which tasks the administrator can perform, for example, by allowing them only to create groups, manage service settings, or reset a user's password.

Customers can strengthen account security by using 2-step verification and security keys.[9] These can help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts.[10] With the Advanced Protection Program for enterprise, we can enforce a curated set of strong account security policies for enrolled users. These include requiring security keys, blocking access to untrusted apps, and enhanced scanning for email threats.

[6] Page 4, How Google Uses Encryption to Protect Your Data
[7] Page 4, How Google Uses Encryption to Protect Your Data
[8] Page 4, Assign administrator roles to a user
[9] Page 4, Protect your business with 2-Step Verification | Further information about deploying 2-step verification can be found on our support page.
[10] Page 4, See security best practices guidance on our security checklists page.

To facilitate easier user access, while at the same time protecting the security of data, Google has developed context-aware access.[11] This provides granular controls for G Suite apps, based on a user's identity and context of the request (such as device security status or IP address). Based on the BeyondCorp[12] security model developed by Google, users can access web applications and infrastructure resources from virtually any device, anywhere, without utilising remote-access VPN gateways while administrators can establish controls over the device.

The protection of information on **mobile and desktop devices** can be a key concern for customers. G Suite customers can use endpoint management[13] to help protect corporate data on users' personal devices and on an organization's company-owned devices. By enrolling the devices for management, users get secure access to G Suite services and organizations can set policies to keep devices and data safe through device encryption and screen lock or password enforcement. Furthermore, if a device is lost or stolen, corporate accounts can be remotely wiped from mobile devices and users can be remotely signed out from desktop devices. Reports enable customers to monitor policy compliance and get information about users and devices. You can obtain further information on endpoint management here.[14]

[11] Page 5, Context-aware access | Integrated with Cloud Identity. Using context-aware access capabilities to protect access to G Suite apps requires a Cloud Identity Premium or G Suite Enterprise license.

[12] Page 5, BeyondCorp

[13] Page 5, Endpoint Management | Included as standard with G Suite.

[14] Page 5, Manage devices for your organization

2.2 Data deletion

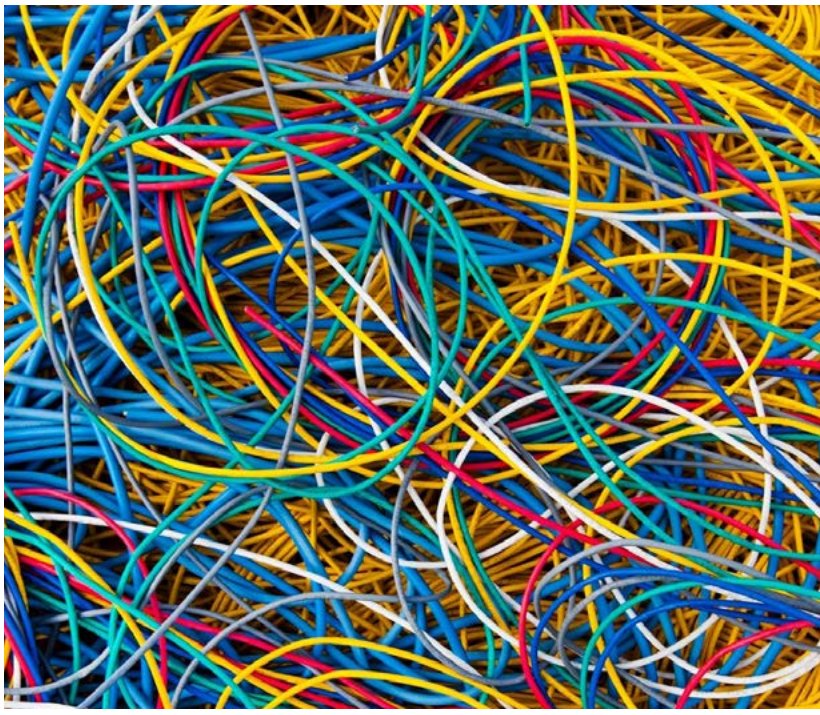
Customers may also seek control over the **deletion of data**. The safe deletion of data is important to customers to protect them from the risk of accidental data loss. At the same time, when customers instruct deletion of data, it is equally important that this data is completely deleted from servers after a period of time.

When you delete data in G Suite, we immediately start the process of removing it from the product and our systems[15] unless it is subject to a Google Vault retention policy per the customer's instructions. First, we aim to immediately remove it from view. We then begin a process designed to safely and completely delete the data from our storage systems. Each Google storage system from which data gets deleted has its own detailed process for safe and complete deletion. This might involve repeated passes through the system to confirm all data has been deleted. Our services also use encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to 6 months.

2.3 Data export and download

Customers may want to export and download their data securely from our services. We provide **portability and migration** capabilities and our specific data portability commitments are included in our data processing agreement.[16]

The data export tool[17] available in your G Suite Admin console enables you to export all supported data for each active user in your organization.[18] We also provide the ability for your users to directly download their data[19] on an individual level.



[15] Page 6, Note that administrators can restore data that was deleted within the past [25] days. Further information is provided on our support page.
[16] Page 6, G Suite Data Processing Amendment
[17] Page 6, Export your organization's data
[18] Customers cannot partially export certain types of data, and cannot export data for a subset of users
[19] Page 6, Download your data

2.4 Data governance

Enterprises operating in certain countries and/or regulated industries, such as Healthcare and Financial Services, may be **required to meet certain compliance obligations**, including HIPAA, PCI DSS, GDPR, etc. By using security settings in G Suite and leveraging the compliance certifications G Suite has achieved, customers can manage their compliance. Section 4.2 of this paper provides an overview of the compliance support that we offer to customers.

Most organizations also have internal policies which dictate the **handling of sensitive data**. To help G Suite administrators maintain control over sensitive data, we offer **information rights management** in Google Drive. Administrators and users can use the access permissions in Google Drive to protect sensitive content by preventing the re-sharing, downloading, printing or copying of the file or changing of the permissions. Administrators can control[20] how users in their organization share Google Drive files and folders. For example, whether users can share files with people outside of their organization or whether sharing is restricted to only trusted domains.[21] Optional alerts can be established to remind users to check that files aren't confidential before they are shared outside of the organization.

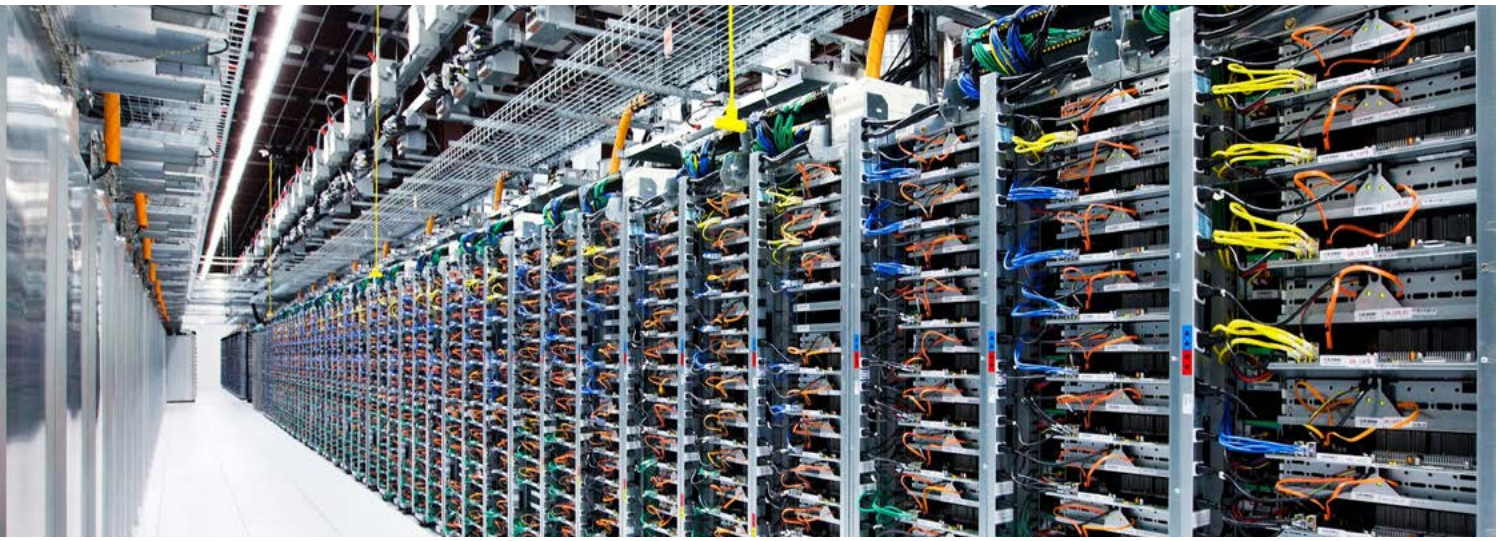
Many organizations are required to **preserve data** for certain periods of time and to delete sensitive data after a time period. Google Vault,[22] the retention solution for G Suite customers, can be used to set retention rules that control how long specific types of data are retained. When retention coverage ends, Vault immediately begins to remove affected data.[23] Customers can create as many custom rules as their organization needs. Learn more[24] about how Vault manages retention.

[20] Page 7, Set Drive users' sharing permissions
[21] Certain features, such as restricting sharing to only whitelisted domains, are only available with G Suite Enterprise, Enterprise for Education, Drive Enterprise, Business, Education, and Nonprofits edition.
[22] Page 7, What is Google Vault? | Included with G Suite Enterprise, Business, Drive Enterprise and G Suite Enterprise for Education editions only.
[23] Refer to section 2.2 Data Deletion for further information about Google's deletion process.
[24] Page 7, How retention works

Data loss prevention (DLP)[25] adds another layer of protection designed to prevent sensitive or private information such as payment card numbers, national identification numbers, or protected health information, from leaking outside of an organization. DLP enables customers to audit how sensitive data is flowing in their enterprise or turn on warning or blocking actions, to prevent users from either **accidentally or maliciously sending confidential data**. To enable this, DLP provides over 100 predefined content detectors, including detection of global and regional identifiers, medical information and credentials. Customers can also define their own custom detectors to meet their enterprise needs. For attachments and image-based documents, DLP uses Google's leading optical character recognition to increase detection coverage and quality. Learn more here about Gmail DLP.[26] DLP can also be used to prevent users from sharing sensitive content in Google Drive or shared drive[27] with people outside of your organization.

Enterprises storing data in the Cloud seek **visibility into data access** and account activity. G Suite audit logs[28] help security teams maintain audit trails in G Suite and view detailed information about Admin activity, data access, and system events. G Suite users can use the Admin Console to access these logs and can customize and export logs as required.

Customers may wish to allow their users **access to third party apps** or may even wish to develop their own custom apps. G Suite has a robust developer ecosystem, with thousands of apps available via G Suite Marketplace and directly to customers, and a rich API framework enabling users to develop custom apps. However, not all third-party apps will conform to every customer's security policy. With app access control,[29] enterprises can see which third-party apps users have approved to access their G Suite data and can reduce this risk by limiting access to trusted apps. We also help enterprises manage risk with app verification,[30] which ensures that apps accessing Gmail data meet security and privacy standards.[31]



[25] Page 8, Google Data Loss Prevention for work | Available to G Suite Enterprise, Drive Enterprise and G Suite Enterprise for Education customers only.
[26] Page 8, Scan your email traffic using DLP rules
[27] Page 8, Scan and protect Drive files using DLP rules
[28] Page 8, Understand audit logs
[29] Available for all G Suite customers
[30] Page 8, Authorize unverified third-party apps
[31] Page 8, Currently, unverified third-party apps with fewer than 100 users worldwide, apps internal to the customer domain, and unverified third-party apps that access data for Google services other than Gmail are not subject to app verification restrictions. Further information for developers is provided in our OAuth API Verification FAQ.

2.5 Data residency

Google's globally distributed data centers[32] reduce latency for multinational organizations and protect their data with geo redundancy. Some organizations, however, have requirements around where their data is stored, and we're committed to meeting their needs.

Data regions[33] for G Suite provides control over the geographical location for storage of email messages, documents, and other G Suite content.[34] Customers can choose between the United States, Europe or global storage. Additionally, data regions offers the flexibility to choose one data region for some of your users, or different data regions for specific departments or teams. Please check this support page[35] for more information on this feature.

2.6 Incident detection & response

With multiple security and privacy controls in place, organizations **need a centralized location where they can prevent, detect, and remediate threats**. The G Suite security center[36] provides advanced security information and analytics, and added visibility and control into security issues affecting your domain.[37] It brings together security analytics, actionable insights and best practice recommendations from Google to empower you to protect your organization, data and users.

As an administrator, you can use the security dashboard to see an overview of different security center reports.[38] The security health page[39] provides visibility into your Admin console settings to help you better understand and manage security risks. Furthermore, you can use the security investigation tool[40] to identify, triage, and take action on security and privacy issues in your domain. Administrators can automate actions in the investigation tool by creating activity rules[41] to detect and remediate such issues more quickly and efficiently. For example, you can set up a rule to send email notifications to certain administrators if Drive documents are shared outside the company.

In addition, the alert center for G Suite[42] provides all G Suite customers with alerts and actionable security insights about activity in your domain to help protect your organization from the latest security threats including phishing, malware, suspicious account, and suspicious device activity. You can also use the alert center API[43] to export alerts into your existing ticketing or SIEM platforms.

Google has a rigorous internal process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data. You can learn more about how Google detects and manages our own incidents in our Data incident response process whitepaper.[44]

[32] Page 9, Discover our data center locations
[33] Page 9, Data regions
[34] Page 9, Refer to this guidance for a list of data and services covered by Data Regions.
[35] Page 9, Choose a geographic location for your data
[36] Page 9, Security centre | Included with G Suite Enterprise edition.
[37] You must be an administrator with a G Suite Enterprise, G Suite Enterprise for Education, Drive Enterprise, or Cloud Identity Premium Edition license to access the security center. With Drive Enterprise or Cloud Identity Premium Edition, you receive a subset of security center reports on the security dashboard.
[38] Page 9, About the security dashboard
[39] Page 9, Get started with the security health page
[40] Page 9, About the security investigation tool
[41] Page 9, Create activity rules with the investigation tool
[42] Page 9, Alert Centre
[43] Page 9, Programmatically manage G Suite alerts.
[44] Page 9, Data incident response process

3. Managing Google's access to your data

This section explains the limited circumstances under which customer data may be accessible by Google personnel and the internal controls to ensure this access is appropriate and limited. The customer contract describes and governs Google's access to customer data. This section further describes the available tools that provide visibility into Google access and the ability to manage and control that access.

3.1 Data access controls

There are three ways customer data may be accessed in G Suite:

1. Direct customer access
2. Internal Google access by authorized individuals
3. Suite service access

Google has three types of controls in place to ensure that each of these access pathways function as intended:

- **Direct customer access:** All authentication sessions to G Suite are encrypted and users can only access the services enabled by their Domain Administrator.
- **Internal Google access by authorized individuals:** Google implements strict access controls to ensure the person accessing the data is authorized to do so and validates that a business justification for access is provided. The justification is made visible to the customer through Access Transparency Logs.[45]
- **G Suite Service Access:** When internal G Suite services access your data, Google uses technologies like Binary Authorization[46] to validate the provenance and integrity of the software.

[45] Page 10, Access Transparency logs | For those services integrated with Access Transparency. Access Transparency is available to G Suite Enterprise and G Suite Enterprise for Education customers only
[46] Page 10, Binary Authorization

3.2 Data access transparency

Google Cloud is explicit in its commitment to customers: **you own your data**, and we will never use it for any purpose other than those necessary to fulfill our contractual obligations. We also know that in addition to commitments, customers want additional transparency and control from their cloud service provider.

As part of Google's long-term commitment to transparency and user trust, we provide **Access Transparency**, a feature that enables customers to **review logs of actions** taken by Google staff when accessing your specific customer data.

Access Transparency log entries include the following types of details: the affected resource and action; the time of the action; the reasons[47] for the action (for example, the case number associated with a customer support request); and data about who is acting on the data (such as the Google staff member's location).

Access Transparency logs are generated when people at Google access data in an Access Transparency supported service (for example, if a Support engineer accesses your data to fix a Calendar problem).[48] G Suite customers can monitor the logs[49] through the G Suite Admin console.

Learn more about Access Transparency for G Suite on this support page.[50]

3.3 Google employee access authorization

Google employees undergo background checks, are required to execute a confidentiality agreement, and comply with Google's code of conduct.[51] In addition, we've designed our systems to **limit the number of employees that have access to customer data** and to **actively monitor** the activities of those employees.

Google employees are only granted a **limited set of default permissions** to access company resources. Access to internal support tools is controlled via **access control lists (ACLs)**. Google follows a formal process to grant or revoke employee access to Google resources, and access is automatically removed for departing employees.

Access authorization is enforced at all relevant layers of the system. Approvals are managed by workflow tools and logged. An employee's authorization settings are used to control access to all resources, including data and systems for G Suite products. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams **actively monitor access patterns and investigate unusual events**.

[47] Page 11, Access Transparency logs
[48] Page 11, There are some exceptions which are detailed in this support article.
[49] Page 11, Access Transparency logs
[50] Page 11, Use Access Transparency to report Google access
[51] Page 11, Google Code of Conduct

3.4 What happens if we get a lawful request from a government for data?

Like other technology and communication companies, Google receives requests from governments around the world to provide subscriber information. Google was the first cloud provider to make public the volume and type of government requests for customer data that we receive in a biannual transparency report,[52] and describe how Google responds to those requests. Our reports are industry-leading and have become the standard in the U.S.

If Google receives a government request for cloud customer data, it is Google's policy to **direct the government to request such data directly from the cloud customer**. Each request that Google receives regarding a customer account is reviewed using these guidelines:

1. **Respect for the privacy and security of data stored with Google.** We have a team that reviews and evaluates each and every one of the requests we receive based on international human rights standards, our own policies, and the law. Google does not provide any government entity with "backdoor" direct access and we do not hesitate to protect customer interests.

2. **Customer notification.** Except in emergency situations involving a threat to life, it is our policy to notify the customer before any information is disclosed unless such notification is prohibited by law.

3. **Consideration of customer objections.** Google will, to the extent allowed by law and by the terms of the request, comply with a customer's reasonable requests regarding its efforts to oppose a request (such as the customer filing an objection to the disclosure with the relevant court and providing a copy of the objection to Google.)

Detailed information is available in our Transparency Report.[53]

[52] Page 12, Requests for user information
[53] Page 12, Requests for user information

4. Security and compliance standards

4.1 Independent verification of our control framework

Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

- **ISO 27001 (Information Security Management)**[54]
- **ISO 27017 (Cloud Security)**[55]
- **ISO 27018 (Cloud Privacy)**[56]
- **SOC 2**[57] and **SOC 3**[58] reports

Google also participates in sector and country-specific frameworks, such as FedRAMP[59] (US government), BSI C5[60] (Germany), MTCS[61] (Singapore), and many others. We also provide resource documents and mappings for certain frameworks where formal certifications or attestations may not be required or applied.

For a complete listing of our compliance offerings, please visit cloud.google.com/security/compliance/.[62]

4.2 Compliance support for customers

Regulations such as GDPR place significant emphasis on enterprises knowing how their data is being processed, who has access to data, and how security incidents will be managed. We have dedicated teams of engineers and compliance experts who support our customers in meeting their regulatory compliance and risk management obligations. Our approach includes **collaborating with customers** to understand and address their specific regulatory needs.

We allow customers in certain regions or customers operating in certain regulated verticals to conduct **audits** to validate Google's security and compliance controls.

[54] Page 13, ISO 27001
[55] Page 13, ISO 27017
[56] Page 13, ISO 27018
[57] Page 13, SOC 2
[58] Page 13, SOC 3
[59] Page 13, FedRAMP
[60] Page 13, Cloud Computing Compliance Controls Catalog (C5)
[61] Page 13, MTCS (Singapore) Tier 3
[62] Page 13, Compliance resource center

5. Conclusion

Protecting customer data is a primary design consideration for Google Cloud's infrastructure, applications and personnel operations. Google's security practices are verified by independent third-parties, providing assurance to customers regarding our security controls and practices. Google offers strong contractual commitments to ensure our customers maintain control over their data and its processing, including the commitment that we only process your customer data according to your instructions

Google Cloud will continue to invest so that customers can use our services in a secure and transparent manner. For more information, please visit cloud.google.com/security/ and to learn more about G Suite security visit gsuite.google.com/security.

Appendix: URLs

Page 3

[2] Privacy: https://cloud.google.com/security/privacy/
[3] How Google Uses Encryption to Protect Your Data: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf
[4] How Google Uses Encryption to Protect Your Data: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf
[5] G Suite (Online) Agreement: https://gsuite.google.com/intl/en_uk/terms/2013/1/premier_terms.html?_ga=2.236109891.-396183558.1551709596&_gac=1.185934747.1566901180.CIODgNiF7-MCFWWOxQIday8BMw

Page 4

[6] How Google Uses Encryption to Protect Your Data: http://services.google.com/fh/files/helpcenter/google_encryptionwp2016.pdf
[7] How Google Uses Encryption to Protect Your Data: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf
[8] Assign administrator roles to a user: https://support.google.com/a/answer/172176
[9] Protect your business with 2-Step Verification: https://support.google.com/a/answer/175197?hl=en
[10] Security checklists : https://support.google.com/a/answer/9184226?hl=en&ref_topic=7559287

Page 5

[11] Context-aware access: https://cloud.google.com/context-aware-access/
[12] BeyondCorp: https://cloud.google.com/beyondcorp/
[13] Endpoint Management: https://gsuite.google.com/products/admin/endpoint/
[14] Manage devices for your organization: https://support.google.com/a/topic/24642?hl=en&ref_topic=4499525

Page 6

[15] Restore a G Suite user's Gmail and Drive data: https://support.google.com/a/answer/6052340?hl=en
[16] G Suite Data Processing Amendment: https://gsuite.google.com/terms/dpa_terms.html
[17] Export your organization's data: https://support.google.com/a/answer/100458?hl=en
[19] Download your data: https://support.google.com/accounts/answer/3024190

Appendix: URLs

Page 7

[20] Set Drive users' sharing permissions: https://support.google.com/a/answer/60781?hl=en
[22] What is Google Vault?: https://support.google.com/vault/answer/2462365?hl=en
[24] How retention works: https://support.google.com/vault/answer/2990828?hl=en#

Page 8

[25] Google Data Loss Prevention for work: https://storage.googleapis.com/gfw-touched-accounts-pdfs/Gmail_dlp_whitepaper.pdf
[26] Scan your email traffic using DLP rules: https://support.google.com/a/answer/6280516?hl=en
[27] Scan and protect Drive files using DLP rules: https://support.google.com/a/answer/6321530?hl=en
[28] Understand audit logs: https://support.google.com/a/topic/9027054
[30] Authorize unverified third-party apps: https://support.google.com/a/answer/9352843?hl=en
[31] OAuth API Verification FAQ: https://support.google.com/cloud/answer/9110914

Page 9

[32] Discover our data center locations: https://www.google.com/about/datacenters/location/
[33] Data regions: https://gsuite.google.com/products/admin/data-regions/
[34] What data is covered by a data region policy?: https://support.google.com/a/answer/9223653?visit_id=637055305974501610-3285746069&rd=1
[35] Choose a geographic location for your data: https://support.google.com/a/answer/7630496?hl=en&ref_topic=7631290
[36] Security centre: https://gsuite.google.com/products/admin/security-center/
[38] About the security dashboard: https://support.google.com/a/answer/7492330
[39] Get started with the security health page: https://support.google.com/a/answer/7491656
[40] About the security investigation tool: https://support.google.com/a/answer/7575955
[41] Create activity rules with the investigation tool: https://support.google.com/a/answer/9275024?hl=en
[42] Alert Centre: https://gsuite.google.com/products/admin/alert-center/
[43] Programmatically manage G Suite alerts: https://developers.google.com/admin-sdk/alertcenter/
[44] Data incident response process: http://services.google.com/fh/files/misc/data_incident_response_2018.pdf

Page 10

[45] Access Transparency logs: https://support.google.com/a/answer/9230979?hl=en&ref_topic=9230579
[46] Binary Authorization: https://cloud.google.com/binary-authorization/

Appendix: URLs

Page 11

[47] Access Transparency logs: https://support.google.com/a/answer/9230979?hl=en&ref_topic=9230579
[48] Use Access Transparency to report Google access: https://support.google.com/a/answer/9230474?hl=en&ref_topic=9230579
[49] Access Transparency logs: https://support.google.com/a/answer/9230979?hl=en&ref_topic=9230579
[50] Use Access Transparency to report Google access: https://support.google.com/a/answer/9230474?hl=en&ref_topic=9230579
[51] Google Code of Conduct: https://abc.xyz/investor/other/google-code-of-conduct/

Page 12

[52] Requests for user information: https://transparencyreport.google.com/user-data/overview
[53] Requests for user information: https://transparencyreport.google.com/user-data/overview

Page 13

[54] ISO 27001: https://cloud.google.com/security/compliance/iso-27001/
[55] ISO 27017: https://cloud.google.com/security/compliance/iso-27017/
[56] ISO 27018: https://cloud.google.com/security/compliance/iso-27018/
[57] SOC 2: https://cloud.google.com/security/compliance/soc-2/
[58] SOC 3: https://cloud.google.com/security/compliance/soc-3/
[59] FedRAMP: https://cloud.google.com/security/compliance/fedramp/
[60] Cloud Computing Compliance Controls Catalog (C5): https://cloud.google.com/security/compliance/bsi-c5/
[61] MTCS (Singapore) Tier 3: https://cloud.google.com/security/compliance/mtcs/
[62] Compliance resource center: https://cloud.google.com/security/compliance/