Google Cloud Security and Compliance Whitepaper

How Google protects your data.

Google Cloud

This whitepaper applies to the following G Suite products

G Suite, G Suite for Education, G Suite for Government, G Suite for Nonprofits, Google Drive, and G Suite Business

Table of Contents

Introduction

Cloud computing offers many advantages and conveniences for today's organizations. Employees can work together in documents in real time from their phone or tablet from any location, and communicate instantly with teammates via video, voice, instant message, or email. No longer tied to a single machine, they have the freedom to work together from anywhere, using any device they choose. Meanwhile, their employers don't shoulder the cost or burden of maintaining servers and constantly updating software. It's no surprise, then, that so many organizations around the world are storing their information and getting work done in the cloud.

The growth of the cloud has thrust the issue of security and trust into the spotlight. That's because cloud services operate very differently from traditional on-premises technology. Rather than residing on local servers, content is now managed on Google servers that are part of our global data center network. In the past, organizations felt that they had complete control over how infrastructure was run and who operated it. Organizations moving to the cloud will rely on cloud suppliers to manage the infrastructure, operations, and delivery of services. In this new world, companies will still control company data, but via cloud-based tools and dashboards. Rather than only using desktop computers, users can now access work files on their personal mobile devices. Customers must assess whether the security controls and compliance of any cloud solution meet their individual requirements. Customers must therefore understand how these solutions protect and process their data. The goal of this whitepaper is to provide an introduction to Google's technology in the context of security and compliance.

As a cloud pioneer, Google fully understands the security implications of the cloud model. Our cloud services are designed to deliver better security than many traditional on-premises solutions. We make security a priority to protect our own operations, but because Google runs on the same infrastructure that we make available to our customers, your organization can directly benefit from these protections. That's why we focus on security, and protection of data is among our primary design criteria. Security drives our organizational structure, training priorities and hiring processes. It shapes our data centers and the technology they house. It's central to our everyday operations and disaster planning, including how we address threats. It's prioritized in the way we handle customer data. And it's the cornerstone of our account controls, our compliance audits and the certifications we offer our customers.

This paper outlines Google's approach to security and compliance for G Suite, our cloud-based productivity suite. Used by more than five million organizations worldwide, from large banks and retailers with hundreds of thousands of people to fast-growing startups, G Suite and G Suite for Education includes Gmail, Calendar, Groups, Drive, Docs, Sheets, Slides, Hangouts, Sites, Talk, Contacts and Google Vault. G Suite is designed to help teams work together in new, more efficient ways, no matter where members are located or what device they happen to be using.

This whitepaper will be divided into two main sections: security and compliance. The security section will include details on organizational and technical controls regarding how Google protects your data. The second section on compliance will cover how your data is processed and details on how organizations can meet regulatory requirements.

Google Has a Strong Security Culture

Google has created a vibrant and inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness.

Employee background checks

Before they join our staff, Google will verify an individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Google may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

Security training for all employees

All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

Internal security and privacy events

Google hosts regular internal conferences to raise awareness and drive innovation in security and data privacy, which are open to all employees. Security and privacy is an ever-evolving area, and Google recognizes that dedicated employee engagement is a key means of raising awareness. One example is "Privacy Week," during which Google hosts events across global offices to raise awareness of privacy in all facets, from software development, data handling and policy enforcement to living our privacy principles. Google also hosts regular "Tech Talks" focusing on subjects that often include security and privacy.

Our dedicated security team

Google employs more than 550 full-time security and privacy professionals, who are part of our software engineering and operations division. Our team includes some of the world's foremost experts in information, application and network security. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure and implementing Google's security policies. Google's dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.

Google employs more than 550 full-time security and privacy professionals, who are part of our software engineering and operations division. Our team includes some of the world's foremost experts in information, application and network security.

Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google's product and engineering teams. They monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.

The security team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Some examples of this research would be the discovery of the POODLE SSL 3.0 exploit and cipher suite weaknesses. The security team also publishes security research papers, available to the public. The security team also organizes and participates in open-source projects and academic conferences.

Our dedicated privacy team

The Google Privacy team operates independently from product development and security organizations, but participates in every Google product launch. The team reviews design documentation and code audits to ensure that privacy requirements are followed. The Privacy team has built a set of automated monitoring tools to help ensure that products with Customer Data operate as designed and in accordance with our privacy policy. They help release products that reflect strong privacy standards: transparent collection of user data and providing users and administrators with meaningful privacy configuration options, while continuing to be good stewards of any information stored on our platform. After products launch, the privacy team oversees automated processes that audit data traffic to verify appropriate data usage. In addition, the privacy team conducts research providing thought leadership on privacy best practices for our emerging technologies.

Internal audit and compliance specialists

Google has a dedicated internal audit team that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties.

Collaboration with the security research community

Google has long enjoyed a close relationship with the security research community, and we greatly value their help identifying vulnerabilities in G Suite and other Google products. Our Vulnerability Reward Program encourages researchers to report design and implementation issues that may put customer data at risk, offering rewards in the tens of thousands of dollars. In Chrome, for instance, we warn users against malware and phishing, and offer rewards for finding security bugs.
Due to our collaboration with the research community, we've squashed more than 700 Chrome security bugs and have rewarded more than $1.25 million — more than $2 million has been awarded across Google's various vulnerability rewards programs. We publicly thank these individuals and list them as contributors to our products and services.

Operational Security

Far from being an afterthought or the focus of occasional initiatives, security is an integral part of our operations.

Vulnerability management

Google administrates a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated.
Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open-source tools. More information about reporting security issues can be found at Google Application Security.

Malware prevention

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network. Google takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware. Google helps tens of millions of people every day to protect themselves from harm by showing warnings to users of Google Chrome, Mozilla Firefox and Apple Safari when they attempt to navigate to websites that would steal their personal information or install software designed to take over their computers. Malware sites or email attachments install malicious software on users' machines to steal private information, perform identity theft, or attack other computers. When people visit these sites, software that takes over their computer is downloaded without their knowledge. Google's malware strategy begins with infection prevention by using manual and automated scanners to scour Google's search index for websites that may be vehicles for malware or phishing. Approximately one billion people use Google's Safe Browsing on a regular basis. Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. In addition to our Safe Browsing solution, Google operates VirusTotal, a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. VirusTotal's mission is to help in improving the antivirus and security industry and make the Internet a safer place through the development of free tools and services.

Google helps tens of millions of people every day to protect themselves from harm by showing warnings to users of Google Chrome, Mozilla Firefox and Apple Safari when they attempt to navigate to websites that would steal their personal information or install software designed to take over their computers.

Google makes use of multiple antivirus engines in Gmail, Drive, servers and workstations to help identify malware that may be missed by antivirus signatures.

Monitoring

Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.

Incident management

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team.

Technology with Security at Its Core

G Suite runs on a technology platform that is conceived, designed and built to operate securely. Google is an innovator in hardware, software, network and system management technologies. We custom-designed our servers, proprietary operating system, and geographically distributed data centers. Using the principles of "defense in depth," we've created an IT infrastructure that is more secure and easier to manage than more traditional technologies.

State-of-the-art data centers

Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs,

activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multifactor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever step foot in one of our data centers.

Powering our data centers

To keep things running 24/7 and ensure uninterrupted services, Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.

Environmental impact

Google reduces environmental impact of running our data centers by designing and building our own facilities. We install smart temperature controls, use "free-cooling" techniques like using outside air or reused water for cooling, and redesign how power is distributed to reduce unnecessary energy loss. To gauge improvements, we calculate the performance of each facility using comprehensive efficiency measurements. We're the first major Internet services company to gain external certification of our high environmental, workplace safety and energy management standards throughout our data centers. Specifically, we received voluntary ISO 14001, OHSAS 18001 and ISO 50001 certifications. In a nutshell, these standards are built around a very simple concept: Say what you're going to do, then do what you say—and then keep improving.

Custom server hardware and software

Google's data centers house energy-efficient custom, purpose-built servers and network equipment that we design and manufacture ourselves. Unlike much commercially available hardware, Google servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities. Our production servers run a custom-designed operating system (OS) based on a stripped-down and hardened version of Linux. Google's servers and their OS are designed for the sole purpose of providing Google services. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer demand. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state.
These automated, self-healing mechanisms are designed to enable Google to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromise on the network.

Hardware tracking and disposal

Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

A global network with unique security benefits

Google's IP data network consists of our own fiber, public fiber, and undersea cables. This allows us to deliver highly available and low latency services across the globe.

In other cloud services and on-premises solutions, customer data must make several journeys between devices, known as "hops," across the public Internet. The number of hops depends on the distance between the customer's ISP and the solution's data center. Each additional hop introduces a new opportunity for data to be attacked or intercepted. Because it's linked to most ISPs in the world, Google's global network improves the security of data in transit by limiting hops across the public Internet.

Google's IP data network consists of our own fiber, public fiber, and undersea cables. This allows us to deliver highly available and low latency services across the globe.

Defense in depth describes the multiple layers of defense that protect Google's network from external attacks. Only authorized services and protocols that meet our security requirements are allowed to traverse it; anything else is automatically dropped. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation. All traffic is routed through custom GFE (Google Front End) servers to detect and stop malicious requests and Distributed Denial of Service (DDoS) attacks. Additionally, GFE servers are only allowed to communicate with a controlled list of servers internally; this "default deny" configuration prevents GFE servers from accessing unintended resources. Logs are routinely examined to reveal any exploitation of programming errors. Access to networked devices is restricted to authorized personnel.

Encrypting data in transit, at rest and backup media

G Suite customers' data is encrypted when it's on a disk, stored on backup media, moving over the Internet, or traveling between data centers. Providing cryptographic solutions that address customers' data security concerns is our commitment. Encryption is an important piece of the G Suite security strategy, helping to protect your emails, chats, Google Drive files, and other data. Additional details on how data is protected at rest, in transit, on backup media and details on encryption key management can be found in our G Suite Encryption Whitepaper.

Low latency and highly available solution

Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and Internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that G Suite customers can continue working in most cases without interruption. Customers with global workforces can collaborate on documents, video conferencing and more without additional configuration or expense. Global teams share a highly performant and low latency experience as they work together on a single global network.

Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages.

Google's highly redundant infrastructure also helps protect our customers from data loss. For G Suite, our recovery point objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in G Suite Products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customer data is divided into digital pieces with random file names. Neither their content nor their file names are stored in readily human-readable format, and stored customer data cannot be traced to a particular customer or application just by inspecting it in storage. Each piece is then replicated in near-real time over multiple disks, multiple servers, and multiple data centers to avoid a single point of failure. To further prepare for the worst, we conduct disaster recovery drills in which we assume that individual data centers—including our corporate headquarters—won't be available for 30 days. We regularly test our readiness for plausible scenarios as well as more imaginative crises,

like alien and zombie invasions.

Our highly redundant design has allowed Google to achieve an uptime of 99.984% for Gmail for the last years with **no scheduled downtime**. Simply put, when Google needs to service or upgrade our platform, users do not experience downtime or maintenance windows.

Service availability

Some of Google's services may not be available in some jurisdictions. Often these interruptions are temporary due to network outages, but others are permanent due to government-mandated blocks. Google's Transparency Report also shows recent and ongoing disruptions of traffic to Google products. We provide this data to help the public analyze and understand the availability of online information.

Independent Third-Party Certifications

Google's customers and regulators expect independent verification of our security, privacy, and compliance controls. In order to provide this, we undergo several independent third-party audits on a regular basis. For each one, an independent auditor examines our data centers, infrastructure, and operations. Regular audits are conducted to certify our compliance with the auditing standards ISO 27001, ISO 27017, ISO 27018, SOC 2 and SOC 3, as well as with the US Federal Risk and Authorization Management Program (FedRAMP). When customers consider G Suite, these certifications can help them confirm that the product suite meets their security, compliance and data processing needs.

ISO 27001

ISO 27001 is one of the most widely recognized and accepted independent security standards. Google has earned it for the systems, technology, processes, and data centers that run G Suite. Our compliance with the international standard was certified by Ernst & Young CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council (a member of the International Accreditation Forum, or IAF). Our ISO 27001 certificate and scoping document are available in here.

ISO 27017

ISO 27017 is an international standard of practice for information security controls based on ISO/IEC 27002 specifically for cloud services. Our compliance with the international standard was certified by Ernst & Young CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council (a member of the International Accreditation Forum, or IAF). Our ISO 27017 certificate is available here.

ISO 27018

ISO 27018 is an international standard of practice for protection of personally identifiable information (PII) in public clouds services. Our compliance with the international standard was certified by Ernst & Young CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council (a member of the International Accreditation Forum, or IAF). Our ISO 27018 certificate is available here.

SOC 2/3

In 2014, the American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC) released the revised version of the Trust Services Principles and Criteria (TSP). SOC (Service Organization Controls) is an audit framework for non-privacy principles that include security, availability, processing integrity, and confidentiality. Google has both SOC 2 and SOC 3 reports. Our SOC 3 report is available for download without a nondisclosure agreement. The SOC 3 confirms our compliance with the principles of security, availability, processing integrity and confidentiality.

FedRAMP

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that is intended to expedite U.S. government agency security assessments and help agencies move to secure cloud solutions. Google maintains a FedRAMP Authorization to Operate (ATO) for Google Apps [G Suite] and App Engine.

Data Usage

Our philosophy

G Suite customers own their data, not Google. The data that G Suite organizations and users put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days. Finally, we provide tools that make it easy for customer administrators to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Google.

No advertising in G Suite

There is **no** advertising in the G Suite Core Services, and we have no plans to change this in the future. Google does not collect, scan or use data in G Suite Core Services for advertising purposes. Customer administrators can restrict access to Non-Core Services from the Google Admin console. Google indexes customer data to provide beneficial services, such as spam filtering, virus detection, spellcheck and the ability to search for emails and files within an individual account.

Data Access and Restrictions

Administrative access

To keep data private and secure, Google logically isolates each customer's G Suite data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies.

Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams.

For customer administrators

Within customer organizations, administrative roles and privileges for G Suite are configured and controlled by the customer. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and data. Integrated audit logs offer a detailed history of administrative actions, helping customers monitor internal access to data and adherence to their own policies.

Law enforcement data requests

The customer, as the data owner, is primarily responsible for responding to law enforcement data requests; however, like other technology and communications companies, Google may receive direct requests from governments and courts around the world about how a person has used the company's services. We take measures to protect customers' privacy and limit excessive requests while also meeting our legal obligations. Respect for the privacy and security of data you store with Google remains our priority as we comply with these legal requests. When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and Google's policies. Generally speaking, for us to comply, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law. If we believe a request is overly broad, we'll seek to narrow it, and we push back often and when necessary. For example, in 2006 Google was the only major search company that refused a U.S. government request to hand over two months of user search queries. We objected to the subpoena, and eventually a court denied the government's request. In some cases we receive a request for all information associated with a Google account, and we may ask the requesting agency to limit it to a specific product or service. We believe the public deserves to know the full extent to which governments request user information from Google. That's why we became the first company to start regularly publishing reports about government data requests. Detailed information about data requests and Google's response to them is available in our Transparency Report. It is Google's policy to notify customers about requests for their data unless

We believe the public deserves to know the full extent to which governments request user information from Google. That's why we became the first company to start regularly publishing reports about government data requests.

specifically prohibited by law or court order.

Third-party suppliers

Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to G Suite, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

Regulatory Compliance

Our customers have varying regulatory compliance needs. Our clients operate across regulated industries, including finance, pharmaceutical and manufacturing.

Google contractually commits to the following:

- Google will maintain adherence to ISO 27001, ISO 27018 and SOC 2/3 audits during the term of the agreement;
- Defined Security Standards. Google will define how data is processed, stored, and protected through specific defined security standards;
- Access to our Data Privacy Officer. Customers may contact Google's Data Privacy Officer for questions or comments;
- Data Portability. Administrators can export customer data in standard formats at any time during the term of the agreement. Google does not charge a fee for exporting data.

Data processing amendment

Google takes a global approach to our commitments on data processing. Google and many of our customers operate in a global environment. G Suite offers a Data Processing Amendment and EU Model Contract Clauses to facilitate compliance with jurisdictional-specific laws or regulations. Your organization can opt into our data processing amendment by following the instructions in our Help Center.

EU Data Protection Directive

The Article 29 Working Party is an independent European advisory body focused on data protection and privacy. They have provided guidance on how to meet European data privacy requirements when engaging with cloud computing providers. Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the Article 29 Working Party.

EU model contract clauses

In 2010, the European Commission approved model contract clauses as a means of compliance with the requirements of the Directive. The effect of this decision is that by incorporating certain provisions into a contract, personal data can flow from those subject to the Directive to providers outside the EU or the European Economic Area. Google has a broad customer base in Europe. By adopting EU model contract clauses, we're offering customers an additional option for compliance with the Directive.

U.S. Health Insurance Portability and Accountability Act (HIPAA)

G Suite supports our customers' compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA), which governs the confidentiality and privacy of protected health information (PHI). Customers who are subject to HIPAA and wish to use G Suite with PHI must sign a business associate agreement (BAA) with Google. The BAA covers Gmail, Google Calendar, Google Drive, Google Sites and Google Vault. Additional information can be found in our HIPAA Implementation Guide.

U.S. Family Educational Rights and Privacy Act (FERPA)

More than 30 million students rely on G Suite for Education. G Suite for Education services comply with FERPA (Family Educational Rights and Privacy Act) and our commitment to do so is included in our agreements.

Children's Online Privacy Protection Act of 1998 (COPPA)

Protecting children online is important to us. We contractually require G Suite for Education schools to obtain parental consent that COPPA calls for to use our services, and our services can be used in compliance with COPPA.

Empowering Users and Administrators to Improve Security and Compliance

Google builds security into its structure, technology, operations and approach to customer data. Our robust security infrastructure and systems become the default for each and every G Suite customer. But beyond these levels, users are actively empowered to enhance and customize their individual security settings to meet their business needs through dashboards and account security wizards. G Suite also offers administrators full control to configure infrastructure, applications and system integrations in a single dashboard via our Admin console — regardless of the size of the organization. This approach simplifies administration and configuration. Consider deployment of DKIM (a phishing prevention feature) in an on-premise email system. Administrators would need to patch and configure every server separately, and any misconfiguration would cause a service outage. Using our Admin console, DKIM is configured in minutes across thousands or hundreds of thousands of accounts with peace of mind and no outage or maintenance window required. Administrators have many powerful tools at their disposal, such as authentication features like 2-step verification and single sign-on, and email security policies like secure transport (TLS) enforcement, which can be configured by organizations to meet security and system integration requirements. Below are some key features that can help customize G Suitefor your security and compliance needs:

User authentication/authorization features

2-step verification

2-step verification adds an extra layer of security to G Suite accounts by requiring users to enter a verification code in addition to their username and password when they sign in. This can greatly reduce the risk of unauthorized access if a user's password is compromised. Verification codes are delivered on a one-time basis to a user's Android, BlackBerry, iPhone, or other mobile phone. Administrators can choose to turn on 2-step verification for their domain at any time.

Security Key

Security Key is an enhancement for 2-step verification. Google, working with the FIDO Alliance standards organization, developed the Security Key — an actual physical key used to access your Google Account. It sends an encrypted signature rather than a code, and helps ensure that your login cannot be phished. Google Cloud admins will be able to easily deploy, monitor and manage the Security Key at scale with new controls in the Admin console with no additional software to install. IT admins will see where and when employees last used their keys with usage tracking and reports. If Security Keys are lost, admins can easily revoke access to those keys and provide backup codes so employees can still sign-in and get work done.

Single sign-on (SAML 2.0)

G Suite offers customers a single sign-on (SSO) service that lets users access multiple services using the same sign-in page and authentication credentials. It is based on SAML 2.0, an XML standard that allows secure web domains to exchange user authentication and authorization data. For additional security, SSO accepts public keys and certificates generated with either the RSA or DSA algorithm. Customer organizations can use the SSO service to integrate single sign-on for G Suite into their LDAP or other SSO system.

OAuth 2.0 and OpenID Connect

G Suite supports OAuth 2.0 and OpenID Connect, an open protocol for authentication and authorization. This allows customers to configure one single sign-on service (SSO) for multiple cloud solutions. Users can log on to third-party applications through G Suite—and vice versa—without re-entering their credentials or sharing sensitive password information.

Data management features

Information Rights Management (IRM)

With Information Rights Management ("IRM") you can disable downloading, printing and copying from the advanced sharing menu — perfect for when the file you're sharing is only meant for a few select people. This new option is available for any file stored in Google Drive, including documents, spreadsheets and presentations created in Google Docs.

G Suite also offers administrators full control to configure infrastructure, applications and system integrations in a single dashboard via our Admin console — regardless of the size of the organization.

Driver audit log

The Driver Audit Log lists every time your domain's users view, create, update, delete, or share Drive content. This includes content you create in Google Docs, Sheets, Slides and other G Suite products, as well as content created elsewhere that you upload to Drive, such as PDFs and Word files.

Drive content compliance / alerting

G Suite has an additional feature that allows Administrators to keep track of when specific actions are taken in Drive and can set up custom Drive alerts. So if you want to know when a file containing the word "confidential" in the title is shared outside the company, now you'll know. And there are more events coming to Drive audit, including download, print and preview alerts.

Trusted domains for drive sharing

G Suite and G Suite for Education administrators will allow for Domain Whitelisting. End users can share to those trusted domains, but can't share to other external domains. Great for partnerships, subsidiaries or other arrangements where certain domains are trusted and users are allowed to share to them.

Email Security features

Secure transport (TLS) enforcement

G Suite administrators can require that email to or from specific domains or email addresses be encrypted with Transport Layer Security (TLS). For instance, a customer organization may choose to transmit all messages to its outside legal counsel via a secure connection. If TLS is not available at a specified domain, inbound mail will be rejected and outbound mail will not be transmitted.

Phishing prevention

Spammers can sometimes forge the "From" address on an email message so that it appears to come from a reputable organization's domain. Known as phishing, this practice is often an attempt to collect sensitive data. To help prevent phishing, Google participates in the DMARC program, which lets domain owners tell email providers how to handle unauthenticated messages from their domain. G Suite customers can implement DMARC by creating a DMARC record within their admin settings and implementing an SPF record and DKIM keys on all outbound mail streams.

Data Loss Prevention (DLP) for Gmail

Gmail data loss prevention (DLP) lets you scan your organization's inbound and outbound email traffic for content, such as credit card or Social Security numbers, and set up policy-based actions when this content is detected. Available actions include sending the message to quarantine, rejecting the message, or modifying the message. If you configure a DLP policy using predefined detectors, the email subject, message body, and attachments are automatically scanned. You can create more sophisticated content compliance policies by combining one or more predefined detectors with keywords or regular expressions to construct compound detection criteria. Sensitive information does not reside exclusively in text documents, but also in scanned copies and images as well. With the new OCR enhancement, DLP policies can now analyze common image types, and extract text for policy evaluation. Admins have the option to enable OCR in the Admin console at the organizational-unit (OU) level for both the Content compliance and Objectionable content rules. Additional information is available in our DLP Whitepaper.

G Suite administrators can require that email to or from specific domains or email addresses be encrypted with Transport Layer Security (TLS).

Email content compliance

Administrators can choose to scan G Suite email messages for predefined sets of words, phrases, text patterns or numerical patterns. They can create rules that either reject matching emails before they reach their intended recipients or deliver them with modifications. Customers have used this setting to monitor sensitive or restricted data, such as credit card information, internal project code names, URLs, telephone numbers, employee identification numbers, and social security numbers.

Objectionable content

The objectionable content setting enables administrators to specify what action to perform for messages based on custom word lists. With objectionable content policies, administrators choose whether messages containing certain words (such as obscenities) are rejected or delivered with modifications; for example, to notify others when the content of a message matches the rules that you set. Administrators can also configure this setting to reject outbound emails that may contain sensitive company information; for example, by setting up an outbound filter for the word *confidential*.

Restricted email delivery

By default, users with Gmail accounts at your domain can send mail to and receive mail from any email address. However, in some cases, administrators may want to restrict the email addresses your users can exchange mail with. For example, a school might want to allow its students to exchange mail with the faculty and other students, but not with people outside of the school. Use the Restrict delivery setting to allow the sending or receiving of email messages only from addresses or domains that administrators specify. When administrators add a Restrict delivery setting, users cannot communicate with anyone, except those authorized. Users who attempt to send mail to a domain not listed will see a message that specifies a policy prohibiting mail to that address, confirming that the mail is unsent. Users receive only authenticated messages from listed domains. Messages sent from unlisted domains—or messages from listed domains that can't be verified using DKIM or SPF records—are returned to the sender with a message about the policy.

eDiscovery features

eDiscovery allows organizations to stay prepared in case of lawsuits and other legal matters. Google Vault is the eDiscovery solution for G Suite that lets customers retain, archive, search and export their business Gmail. Administrators can also search and export files stored in Google Drive.

Email retention policy

Retention rules control how long certain messages in your domain are retained before they are removed from user mailboxes and expunged from all Google systems.
G Suite allows you to set a default retention rule for your entire domain. For more advanced implementations, Google Vault allows administrators to create custom retention rules to retain specific content. This advanced configuration allows administrators to specify the number of days to retain messages, whether to delete them permanently after their retention periods, whether to retain messages with specific labels, and whether to let users manage email deletion themselves.

Legal holds

Google Vault allows administrators to place legal holds on users to preserve all their emails and on-the-record chats indefinitely in order to meet legal or other retention obligations. You can place legal holds on all content in a user's account, or target specific content based on dates and terms. If a user deletes messages that are on hold, the messages are removed from the user's view, but they are not deleted from Google servers until the hold is removed.

Search/discovery

Google Vault allows administrators to search Gmail and Drive accounts by user account, organizational unit, date or keyword. Search results include email, on-the-record chats, Google file types and non-Google file types such as PDF, DOCX and JPG.

Evidence export

Google Vault allows administrators to have the ability to export specific email, on-the-record chats and files to standard formats for additional processing and review in a manner that supports legal matters while respecting chain of custody guidelines.

Support for third-party email platforms

The comprehensive mail storage setting ensures that a copy of all sent or received mail in your domain—including mail sent or received by non-Gmail mailboxes—is stored in the associated users' Gmail mailboxes. For organizations that reroute mail to non-Gmail mail servers, this setting also ensures storage of mail in Gmail mailboxes for archiving and eDiscovery purposes.

Securing endpoints

Mobile device management (MDM)

Mobile device management in G Suite eliminates the need for on-premises device or third-party management solutions. Administrators can enforce policies over mobile devices in their organization, encrypt data on devices, and perform actions like remotely wiping or locking lost or stolen devices. This type of control helps ensure the security of business data, even if employees choose to work on their personal phones and tablets. Mobile device management in G Suite works with Android, iOS, Windows Phone, and smartphones and tablets using Microsoft Exchange ActiveSync, such as BlackBerry 10.

Policy-based Chrome browser security

All of the tools and features in G Suite are best supported by Google Chrome. **Administrators can apply security and usage policies across Windows, OSX, Linux, iOS, and Android.** Chrome's standard security features include Safe Browsing, sandboxing, and managed updates that protect users from malicious sites, viruses, malware, and phishing attacks. There are also measures in place to prevent cross-site scripting, which attackers can use to steal private data. G Suite administrators can deploy Google Chrome across their organization and customize it to meet their needs.

Administrators can enforce policies over mobile devices in their organization, encrypt data on devices, and perform actions like remotely wiping or locking lost or stolen devices.

Over 280 policies help administrators control how employees use Chrome across devices. For example, administrators can enable automatic updates to get the latest security fixes, block or allow specific apps, and configure support for legacy browsers.

Chrome device management

The Google Admin Console applies policy to Chrome devices such as Chromebooks, Chromeboxes, and Chromebox for Meetings, which are fast, secure, and cost-effective computers that run Chrome as an operating system. Administrators can easily manage security and other settings for their organization's Chrome devices from a single place. They can configure Chrome features for their users, set up access to VPNs and WiFi networks, pre-install apps and extensions, restrict sign-in to certain users, and more.

An administrator can restore a user's Drive or Gmail data for up to 25 days after date of deletion. After 25 days, Google permanently deletes the user data, and it can't be restored, even if you contact technical support.

Data Recovery

Restore a recently deleted user

An administrator can restore a deleted user account for up to five days after date of deletion. After five days, the Admin console permanently deletes the user account, and it can't be restored, even if you contact Google technical support. Please note that only customer Administrators can delete accounts.

Restore a user's Drive or Gmail data

An administrator can restore a user's Drive or Gmail data for up to 25 days after the data is removed from the user's trash. After 25 days, the data cannot be restored, even if you contact technical support. Google will delete all Customer-deleted data from its systems as soon as reasonably practicable and within a maximum period of 180 days.

Security reports

G Suite administrators have access to security reports that provide vital information on their organization's exposure to data compromise. They can quickly discover which particular users pose security risks by eschewing 2-step verification, installing external apps, or sharing

documents indiscriminately. Administrators can also choose to receive alerts when suspicious login activity occurs, indicating a possible security threat.

Conclusion

The protection of user data is a primary design consideration for all of Google's infrastructure, applications and personnel operations. Protection of user data is far from being an afterthought or the focus of occasional initiatives, it's an integral part of what we do. We believe that Google can offer a level of protection that very few can match. Because protecting your data is part of our core business, Google can develop security innovations such as 2-step authentication and stronger encryption methods. We are able to make extensive investments in security, resources and expertise at a scale that few can afford. Our scale of operations and collaboration with the security research community enable Google to address vulnerabilities quickly or prevent them entirely. Google's security and operational procedures are verified by independent third-party auditors.

Data protection is more than just security, Google offers strong contractual commitments in our Data Processing Amendment to make sure our customers maintain control over the data and how it is processed, including the assurance that your data in the G Suite Core Services is used for the purposes specified in your agreement, and not used for advertising.

For these reasons and more over 5 million organizations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue to invest in security, innovation to evolve our platform to allow our users to benefit from our services in a secure and transparent manner.

Data protection is more than just security. Google offers strong contractual commitments in our Data Processing Amendment to make sure our customers maintain control over the data and how it is processed, including the assurance that your data in the G Suite Core Services is used for the purposes specified in your agreement, and not used in advertising.