

## Overview

Google's security strategy provides controls at multiple levels of data storage, access, and transfer. The strategy includes the following ten components:

- Google corporate security policies
- Organizational security
- Data asset management
- Access control
- Personnel security
- Physical and environmental security
- Infrastructure security
- Systems and software development and maintenance
- Disaster recovery and business continuity

## Office of Information Security Assessment Process

The Office of Information Security (OIS) performed a comprehensive assessment of the Google Apps for Government solution. The assessment process involved a NDA review of multiple internal Google documents and processes by the Colorado State Chief Information Security Officer (CISO) with the Google CISO and Google security staff.

The State CISO reviewed and validated the 300+ page Google Federal System Security Plan (SSP) required by the federal government. The purpose of the system security plan (SSP) is to provide an overview of the security requirements of the system and describe the security controls in place or planned, responsibilities and expected behavior of all individuals who access the Google Apps for Government solution. SSP summary information can be requested by contacting [CISO@state.co.us](mailto:CISO@state.co.us).

The initial assessment found Google Apps for Government to be compliant with OIS and Federal security requirements. The following section provides a summary of the validated security program and security controls implemented and maintained by Google.

## Google Corporate Security Policies

Google's security policies cover a wide array of security related topics ranging from general policies that every employee must comply with such as account, data, and physical security, along with more specialized policies covering internal applications and systems that employees are required to follow.

These security policies are periodically reviewed and updated. Employees are also required to receive regular security training on security topics such as the safe use of the Internet, working from remote locations safely, and how to label and handle sensitive data. Additional training is routinely given on policy topics of interest, including in areas of emerging technology, such as the safe use of mobile devices and social technologies.

## Organizational Security

Google's security organization is broken down into several teams that focus on information security, global security auditing, and compliance, as well as physical security for protection of Google's hardware infrastructure. These teams work together to address Google's overall global computing environment.

### Information Security Team

Google employs a full-time Information Security Team that is composed of over 250 experts in information, application, and network security. This team is responsible for maintaining the company's perimeter and internal defense systems, developing processes for secure development and security review, and building customized security infrastructure. It also has a key role in the development, documentation, and implementation of Google's security policies and standards.

### Global Internal Audit and Global Compliance Team

In addition to a full-time information security team, Google also maintains several functions focused on complying with statutory and regulatory compliance worldwide.

Google has a Global Compliance function that is responsible for legal and regulatory compliance as well as a Global Internal Audit function responsible for reviewing and auditing adherence to said compliance requirements, such as Sarbanes-Oxley and Payment Card Industry standards (PCI).

### Physical Security Team

Google maintains a global team of staff, headquartered in the United States, dedicated to the physical security of Google's office and data center facilities.

Google's security officers are qualified with training to protect high security enterprises with mission-critical infrastructures.

## Data Asset Management

Google's data assets - comprising customer and end-user assets as well as corporate data assets - are managed under security policies and procedures. In addition to specific controls on how data is handled, all Google personnel handling data assets are also required to comply with the procedures and guidelines defined by the security policies.

### Information Access

Google has controls and practices to protect the security of customer information. The layers of the Google application and storage stack require requests coming from other components are authenticated and authorized. Service-to-service authentication is based on a security protocol that relies on authentication infrastructure built into the Google production platform to broker authenticated channels between application services.

For example, a Google web application front-end might receive an end-user authenticated external request to display user data. The front-end in turn makes a remote procedure call to an application back-end to process the request. This remote procedure call is authenticated by the back-end, and will only be

processed if the caller is authenticated as an authorized front-end application. If authorized, the application back-end will make a remote procedure call to a storage layer to retrieve the requested data. The storage layer again authenticates and authorizes the request, and will only process the request if the requester (the service back-end) is authenticated as authorized to access to the data store in question.

Access by production application administrative engineers to production environments is similarly controlled. A centralized group and role management system is used to define and control engineers' access to production services.

### **Data and Access Protection**

Administrative access to the production environment for debugging and maintenance purposes is based on secure shell (SSH) connections. SSH connections into the production environment are authenticated using short-lived public-key certificates that are issued to individual administrative users; issuance of such certificates is in turn authenticated via two-factor authentication.

Customer access to Google Apps for Government is accomplished through SSL protected connections.

Google provides many services that make use of the Hypertext Transfer Protocol Secure (HTTPS) for more secure browser connections. Services such as Gmail, Google Search, and Google+ support HTTPS by default for users who are signed into their Google Accounts. Information sent via HTTPS is encrypted from the time it leaves Google until it is received by the recipient's computer.

### **Email Encryption**

Google Message Discovery, powered by Postini, is a secure, hosted service that provides automated and end-user driven email and attachment encryption capabilities to protect sensitive data and email communication.

Reference: <http://www.google.com/postini/>

### **Archiving and E-Discovery**

Google Message Discovery, powered by Postini, provides comprehensive email archiving and message discovery capabilities. Google Message Discovery allows the state to:

- create a centralized and searchable email repository for the state
- quickly search across the archive to find emails and save result sets
- set central email policies to manage content and compliance requirements

### **HIPAA Data At-Rest Encryption**

Google already provides several means of industry leading security layers to keep Protected Health Information (PHI) confidential and private as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

As an added level of protection, OIT will be implementing an encryption solution for state HIPAA entities, called CipherCloud, to encrypt all email's (subject, body, and attachments) on the way to Google's servers,

so the contents are secure and can't be accessed by anyone outside the state while the email is stored within the Google Apps for Government cloud. Colorado is the first state in the nation to implement this solution.

### **Media Disposal**

When retired from Google's systems, disks containing customer information are subjected to a data destruction process before leaving Google's premises. First, their policy requires the disk to be logically wiped by authorized individuals using a process approved by the Google Security Team and meets DOD sanitization requirements.

Next, another authorized individual is required to perform a second inspection to confirm the disk has been successfully wiped. These erase results are logged by the drive's serial number for tracking.

Finally, the erased drive is released to inventory for reuse and redeployment. If the drive cannot be erased due to hardware failure, it must be securely stored until it can be physically destroyed. Each facility is audited on a weekly basis to monitor compliance with the disk erase policy.

### **Access Control**

Google employs a number of authentication and authorization controls that are designed to protect against unauthorized access.

#### **Authentication Controls**

Google requires the use of a unique User ID for each employee. This account is used to identify each person's activity on Google's network, including any access to employee or customer data. This unique account is used for every system at Google. Google makes widespread use of two-factor (2-step) authentication mechanisms, such as certificates and one-time password generators. Two-factor authentication is required for all access to production environments and resources through Google's Single Sign On system.

Two-factor authentication will be required for customer access to Google Apps for Government through a web browser.

#### **Authorization Controls**

Access rights and levels are based on a Google employee's job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities.

Google Apps for Government provides a feature rich set of access controls for customer access and sharing of resources. Audit capabilities exist to ensure the integrity and effectiveness of access controls implemented through the customer portal.

### **Personnel Security**

Google employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

Upon hire, Google verifies an individual's education and previous employment, and performs internal and external reference checks. Where local labor law or statutory regulations permit, Google also conducts criminal, credit, immigration, and security checks.

All Google staff, who access and maintain Google Apps for Government, are required to pass and maintain a Federal GSA approved background check, to include fingerprints.

## Physical Security

Google has policies, procedures, and infrastructure to handle both physical security of its data centers as well as the environment from which the data centers operate.

Google's data centers are geographically distributed and employ a variety of physical security measures. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks. The standard physical security controls implemented at each Google data center include the following: custom designed electronic card access control systems, alarm systems, interior and exterior cameras, and security guards.

Google has released a seven-minute video to demonstrate their level of security, data protection and server reliability protocols Google follows at their data centers to protect its customers.

Reference: Google Data Center Security Video

<http://youtu.be/1SCZzgdTBo>

## Infrastructure Security

Google security policies and practices provide a series of threat prevention and infrastructure management procedures.

## Malware Protection

Google takes malware threats to its networks and its customers very seriously and uses a variety of methods to address malware risks. This strategy begins with manual and automated scanners that analyze Google's search index for websites that may be vehicles for malware or phishing. This threat information is integrated into internal security threat protection controls and processes. Additionally, Google utilizes use of anti-virus software and proprietary techniques in Gmail, on servers, and on workstations to address malware.

Google Message Discovery, powered by Postini, provides enterprise-grade spam and virus protection to all Gmail users.

## Monitoring

Google's security monitoring program analyzes information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. At multiple 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 unexpected activity in former employees' accounts or attempted access of customer data.

### **Vulnerability Management**

Google employs a team that has the responsibility to manage vulnerabilities in a timely manner. The Google Security Team scans for security threats using commercial and in-house-developed tools, automated and manual penetration efforts, quality assurance (QA) processes, software security reviews, and external audits. The vulnerability management team is responsible for tracking and managing vulnerabilities throughout the Google Apps for Government and Corporate infrastructures.

### **Incident Management**

Google has an incident management process for security events that may affect the confidentiality, integrity, or availability of its systems or data. This process specifies courses of action and procedures for notification, escalation, mitigation, and documentation.

Google 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 identified areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities.

The Google incident management process will be tied into the State of Colorado incident management process.

### **Network Security**

Google employs multiple layers of defense to help protect the network perimeter from external attacks. Only authorized services and protocols that meet Google's security requirements are permitted to traverse the company's network. Unauthorized packets are automatically dropped.

### **Operating System Security**

Based on a proprietary design, Google's production servers are based on a version of Linux that has been customized to include only the components necessary to run Google applications, such as those services required to administer the system and serve user traffic. The system is designed for Google to be able to maintain control over the entire hardware and software stack and support a secure application environment.

Google servers are 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. Using a change management system to provide a centralized mechanism for registering, approving, and tracking changes that impact all systems, Google reduces the risks associated with making unauthorized modifications to the standard Google OS.

## System Development and Maintenance

It is Google's policy to consider the security properties and implications of applications, systems, and services used or provided by Google throughout the entire project lifecycle. Google's "Applications, Systems, and Services Security Policy" calls for teams and individuals to implement appropriate security measures in applications, systems, and services being developed, commensurate with identified security risks and concerns. The policy states that Google maintains a security team chartered with providing security-related guidance and risk-assessment.

## Security Consulting and Review

With regards to the design, development, deployment, and operation of applications and services, the Google Security Team provides the following primary categories of consulting services to Google's Product and Engineering Teams:

- **Security Design Reviews** — design-level evaluations of a project's security risks and corresponding mitigating controls, as well as their appropriateness and efficacy.
- **Implementation Security Reviews** — implementation-level evaluation of code artifacts to assess their robustness against relevant security threats.
- **Security Consulting** — ongoing consultation on security risks associated with a given project and possible solutions to security concerns, often in the form of an exploration of the design space early in project life cycles.

## Software Security Lifecycle Management

Security is a key component of Google's design and development process. Google's Engineering organization does not require Product Development teams to follow a specific software development process; rather, teams choose and implement processes that fit the project's needs. As such, a variety of software development processes are in use at Google, from Agile Software Development methodologies to more traditional, phased processes. Google's security review processes are adapted to work within the chosen framework.

Engineering management has defined requirements for project development processes:

- Peer-reviewed design documentation
- Adherence to coding style guidelines
- Peer code review
- Multi-layered security testing

The Google Security Team's software engineers collaborate with other engineers across Google on the development and vetting of reusable components designed and implemented to help software projects avoid certain classes of vulnerabilities.

### **Security Education**

Recognizing the importance of an engineering workforce that is educated with respect to secure coding practices, the Google Security Team maintains an engineering outreach and security education program.

### **Implementation-Level Security Testing and Review**

Google employs a number of approaches intended to reduce the incidence of implementation-level security vulnerabilities in its products and services:

- Implementation-level security reviews, which are conducted by members of the Google Security Team typically in later stages of product development, aim to validate that a software artifact has protection against relevant security threats.
- Automated testing for flaws in certain relevant vulnerability classes. We use both in-house developed tools and some commercially available tools for this testing.
- Security testing performed by Software Quality Engineers in the context of the project's overall software quality assessment and testing efforts.

### **Disaster Recovery and Business Continuity**

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implements a disaster recovery program at all of its data centers. This program includes multiple components to minimize the risk of any single point of failure, including the following:

- Data replication and backup: Google application data is replicated to multiple systems within a data center, and in some cases also replicated to multiple
- data centers.
- Google operates a geographically distributed set of data centers that is designed to maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between the data centers help to support swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage, and system administration.