MADISON METROPOLITAN SCHOOL DISTRICT

TECHNICAL SERVICES

545 West Dayton St. ● Madison, Wisconsin 53703-1995 ■ 608.663.5430 ▼ www.mmsd.org

Mark H. Evans, *Director*

Daniel A. Nerad, *Superintendent of Schools*

APPENDIX LLL-12-20
June 14, 2010

DATE: **June 7, 2010**

Draft

TO: **BOARD OF EDUCATION**

FROM: **Mark H. Evans, Dir.: Technical Services Division**

RE: Request BOE Approval to replace both our student and staff email systems

1. **Project Title:** Replace both student and staff email systems

2. **Project Description:** Replace both student and staff email systems

3. **Analysis:** Technical Services has planned to replace our Eudora student email system since 2008 and identified this as Activity 50 in the June 2010 Technology Plan, approved by the Board of Education. Consideration has also been given to replacing our GroupWise staff email system since instability of the web version of this system became a problem beginning in October 2009. Demands on our staff email system have always been greater due to our need for highly secure, robust and reliable local and remote access, shared calendaring, and integration with an archival system allowing for a seven year retention. This has been a complicated system and is core to many critical business and legal functions of the District.

   An request for proposals (RFP) for alternatives to replace our student email, with the caveat that our staff email might be considered as well, was released in fall 2009, generating responses from nine vendors, representing 11 products. Both Microsoft's Live@edu and Google's Gmail have been final contenders for student email and following product reviews in March by 13 teachers, six technical staff and four administrators, consensus built around migrating both student and staff email to Gmail. In addition to email, Google Apps for Education includes access to a wide variety of Google tools including Docs (word processing, spreadsheets, presentations, forms) and Google calendar.

   Financial considerations:

   - Moving to Gmail for both students and staff will enable free email account hosting and cost $67,320/yr for the use of Postini for staff email archiving. We will continue to use Novell's ZenWorks for desktop application maintenance, at a cost of $28,000/yr through the 2010-2011 fiscal year. This approach would cost $95,320/yr. Discussion around creating and maintaining Gmail accounts from Infinite Campus and Lawson, as well as migrating staff calendars and live email accounts has not concluded whether consulting help will be required, although discussions with other school districts suggest we may not need external assistance. Should technical assistance be required we would hire consulting support on a time and materials basis, for this help.

   - If instead, the District stayed with GroupWise bundled with ZenWorks, Novell's annual maintenance would be $54,378/yr. Continuing use our current staff email archive product would cost $29,300/yr. This approach would cost $83,678/yr, an annual savings of less than $12,000. However, this approach will continue to require growth in data storage and requires an estimated 0.5 FTE allocation to maintain.

   Migrating both student and staff email to Gmail is compelling for an overall financial perspective when storage and support costs are considered. The Postini archival solution with Gmail has performed adequately

for other K-12 districts and meets their legal requirements. Google provides a template for planning a migration to Gmail which we intend to follow. Some external technical support may be needed, but our intent to use internal staff to the maximum extent possible. Staff time saved by moving to a Gmail solution would be reallocated to other critical Technical Services initiatives including implementation and support of our wireless and thin client/virtual desktop projects.

Other issue:

- Eliminating use of GroupWise would eliminate staff access to the current web version to personal GroupWise email archives. However, we may be able to create an alternative interface or enable one with the help of a third party. Technical Services is investigating this and will provide some method of access.

- Existing staff email archives will be maintained for legal searches for seven years. No maintenance would be paid to Messaging Architects for this since no new archives would be added and no software upgrades would be required.

- We plan to use site based "Google teams" to assist with training a roll out in schools. Our teams would include staff, parents, and students. Training would occur in August as school begins to resume.

- Attached is the frequently asked questions (FAQ) published by Google for districts considering a migration to Gmail as well as their information regarding data privacy and security.

4. **Applicable Board Policies:** N/A

5. **Advertising/Notices/Invites:** Request for proposals (RFP) released in December 2009

6. **Vendors Receiving RFP:** Nine vendors responded

7. **Bids Respondents:** See #6

8. **Estimate:** $67,320 to Google for Postini; $28,000 to Novell for ZenWorks

9. **Previous Fiscal Year Expenditures:** $29,300 for GWArchive from Messaging Architects; $54,378 to Novell for ZenWorks bundled with GroupWise

10. **Funding Source:** Technical Services Division operating budget with prorated allocations coming from Cy Pres buildings in the Microsoft Settlement

11. **Project Schedule:** June 2010

12. **Contract Compliance:** in process

13. **Recommendation:** It is recommended payment be made to Google for use of Postini in the amount of $67,320 and a payment be made to Novell in the amount of $28,000 for use of ZenWorks. Funding comes from the 2010-11 Technical Services Division operating budget with prorated allocations coming from Cy Pres buildings in the Microsoft Settlement.

Google Apps Google Apps Admin Help Search Help

Find more apps for Google Apps on the Google Apps Marketplace Hide

Education Edition - Common Questions

Here is a list of commonly asked questions about Google Apps Education Edition. For additional information, please go to the Google Apps Education Edition website.

General Information

1) What is Google Apps Education Edition?

Google is currently offering schools a hosted solution for their email, calendar, and chat through Google Apps Education Edition, our integrated communication and collaboration solution. Our offer includes Gmail, Google Calendar, Google Talk, Google Sites, and Google Docs and Google Video, all using your own school's domain.

Google Apps Education Edition includes:

- **Gmail:** Email storage and search tools that help your students find information fast and instant messaging from right inside their accounts.
- **Google Calendar:** Students can organize their schedules and share events and calendars with others.
- **Google Talk:** Students can call or send instant messages to their contacts for free anytime, anywhere in the world.
- **Google Docs:** Share documents, spreadsheets, and presentations. Collaborate in real-time with your team or with your whole school. You can publish final documents to the entire world, too.
- **Google Sites:** Work together to keep related documents, web content and other information in one place, on one site.
- **Google Video for education:** A video hosting and sharing solution that enables schools and other organizations to use video as an effective medium for internal communication and collaboration.

2) Why Google Apps?

3) What other schools are using Google Apps for Education?

4) How much is Google Apps for Education?

Google Apps for Education is free. We plan to keep the core offering of Google Apps Education Edition free. This includes user accounts for incoming students in the future. As you may know, Google was founded by a research project at Stanford University, and this is just one way we can give back to the educational community.

To see the available features included in Google Apps Education Edition please navigate here.

For more information, you can review our Terms of Service.

If you would like to purchase Google Message Security and Compliance for filtering or archiving purposes, this will have a per user fee depending on the services you choose. Each package is listed here.

5) Will there be advertisements with Google Apps?

There are no advertisements used with the Google Apps Education Edition.

If you have an account for only alumni at your schools, you are required to enable advertisements.

Gmail also offers web clips at the top of your inbox which show you news headlines, blog posts, RSS and Atom feeds, and relevant sponsored links. Each clip displays the source from which it was received, how long ago the clip was published, and a link to access the entire story or page containing the clip. You may want to create custom RSS feeds for your University.

If you have an Education domain and choose to Hide all advertisements for this domain in your domain's Google Apps control panel, then sponsored links will also no longer be shown as webclips. Your users will still be able to customize their webclips for news headlines, blog posts, RSS feeds, and Atom feeds.

6) How much storage do users get with Google Apps Education Edition?

Each service has different limits associated with it. Please see below:

- Mail: Each user has over 7GB of storage
- Docs
- Video
- Sites

7) What is the uptime for the Google Apps email?

With Google Apps Education Edition, GMail, Google Calendar, Google Talk, Google Docs, and Google Sites are guaranteed to be available at least 99.9% of the time, ensuring that users have access when they need it. The Google Apps team is committed to providing your school with the best level of service. For more information, please go here.

8) What's the difference between Education Edition and Premier Edition?

Here is a comparison chart of Education Edition vs. Premier Edition:

	Education Edition	Premier Edition
Cost	Free!	$50/user/year
Google Video	10GB	3GB
Google Sites	100GB	10Gb + 500Mb*# of paid users
Message Security -Powered by Postini	Free for K-12 schools	Free for all Premier users
Email Storage	7.3 GB	25 GB

9) How secure is Google Apps?

Two of the most common topics of questions regarding Google in general, and Google Apps specifically, are security and privacy. We take both topics very seriously and truly believe that our offerings are a great option for customers on both fronts.

Our business is built on our users' trust: trust in our ability to properly secure their data and our commitment respect the privacy of the information they place in our systems by not giving that information to others or using it inappropriately.

We have an additional FAQ page regarding these topics and this can be found here.

10) Are nonprofit organizations eligible for Education Edition?

Accredited US 501(c)(3) non-profit organizations with under 3,000 users are eligible for Education Edition. If your nonprofit organization is over 3,000, you are eligible for Google Apps Premier Edition at a 40% discount ($30/user/year). Learn more.

If you're a non-profit organization over 3,000 that had already upgraded to Education Edition prior to August 2009, this change will not affect you.

11) What is Google Message Security for K-12?

To help address schools' email security needs, Google Message Security (GMS) is now offered free to current and new eligible K-12 Google Apps Education Edition domains that opt-in to the service by July 2010. See below for details on how to enable GMS for your domain. For more information, please go here.

12) Do I qualify for the free Google Message Security promotion?

The promotion is currently offered to primary or secondary educational institutions that are officially accredited to

provide compulsory education. For more information, please go here.

Signing Up

1) How do I sign up for Google Apps Education Edition?

If you'd like to sign up for Google Apps Education Edition, please visit the sign-up page to register.

Once you've signed up Google Apps Education Edition, you can activate your services by verifying domain ownership. For an overview of the set up process and step by step instructions, visit http://www.google.com/a/help/intl/en/admins/resources/setup/.

You can sign up yourself with the above information or contact sales for additional information. You can contact the sales team at www.google.com/a/edu.

If you need help setting up your account, Google Apps offers partners that can assist you with your deployment. You can contact partners at our Enterprise Solutions Marketplace.

We would also recommend going to this site to understand a good overview of project planning to deploy Google Apps.

2) How to I upgrade my account to the Education Edition?

To qualify for the free Education Edition, we require that organizations meet either of the following criteria:

- K-12 or higher educational institution, non-profit, accredited by a generally accepted accreditation body
- U.S. non-profit organization with current 501(c)(3) status and fewer than 3,000 users.

Note: U.S. non-profit organizations with more than 3,000 users qualify for Premier Edition at only $30/user/year, a 40% discount - sign up here.

Student/alumni/parent groups, religious organizations, home schools or government bodies that are not registered as 501(c)(3) do not qualify for the Education Edition.

If you are an alumni association associated, church school or research lab associated with an accredited school, this qualifies for the Education edition. The easiest way is to sign up under a school's domain.

We're working hard to expand the availability of the Education Edition to international non-profits, so please stay tuned. In the mean time, international non-profits are welcome to sign up for Google Apps Standard Edition or Premier Edition, both currently available in many languages worldwide.

If you think your organization qualifies, please click here to upgrade your domain:

Deploying Google Apps

1) How long does it take to implement Google Apps?

On average, it takes 6 weeks to deploy Google Apps. For a general outline of project timeline, please go here. This project plan will help guide you to a successful deployment.

2) Can existing email data be migrated to Google Apps?

Yes, We provide a range of email migration options to allow you to migrate your old email to Google Apps as described here.

3) Can my school's existing authentication system to integrate with Google Apps?

Yes, Google Apps offers the Single Sign-on API that uses SAML 2.0 to integrate with your authentication system. Google Apps also offers an extensive code library for your reference while setting this up. For details about the SSO API, please navigate to the SSO API section of the Code site.

4) How many accounts can I get with Google Apps? Do I have to delete inactive users?

The number of users you can have on Google Apps Education edition is practically limitless (as long as you aren't

generating spam). You can request more user accounts via the control panel interface. In addition to that, we do not require you to delete inactive users.

5) How do I monitor/ filter/archive data with Google Apps Education Edition?

Google Apps for Education gives schools the ability to filter, monitor or archive mail using our Google Message Security and Compliance Solutions.

You can learn more about these solutions here.

We offer a 66% discount for K-12 educational institutions.

Alternatively you could choose to implement your own filtering, monitoring or archiving solution using an email gateway. This gateway allows your school to route all mail into and out of our system through your network. This gives you the ability to filter, monitor, and archive in any way you see fit.

We have developed a guide on how to implement a Mail Gateway, for more details , see this page.

We have a number of partners who can offer this service if you do not want to implement it yourself. You can navigate here learn more about the partners.

6) How do I train faculty and students how to use Google Apps?

We offer many resources such as online presentations and Help Centers to help you train your users to use Google Apps. To access this information, you can go here. If you need additional training, our partners also offer this service. More details can be found at the Enterprise Solutions Marketplace.

7) What happens if I have a problem?

The Google Apps Administrators Help Center is a great resource to troubleshoot any problems that you have. If you cannot find the answer online, we offer phone support and priority email for Google Apps Education Edition customers.

Google Apps offers phone support for Education Edition customers for issues that pertain to a service that is unusable. We define 'unusable' as a Google server error that prevents one or more users from accessing a Google Apps online service. Hours of operation are Sunday 5 p.m. Pacific Standard Time until Friday 5 p.m. Pacific Standard Time. All other issues will be efficiently supported via email.

Please navigate here for more information about how to access phone support and priority email.

updated 5/10/2010

Was this information helpful? ○ Yes ○ No

Tell us how we're doing: Please answer a few questions about your experience to help us improve our Help Center.

Google

Comprehensive review of security and vulnerability protections for Google Apps

A Google white paper February 2007

Security of Google Apps

Google

FOR MORE INFORMATION

Online www.google.com/a
Email apps-enterprise@google.com

Securing network-based applications against would-be hackers is key to ensuring the success of any system. When it comes to email and collaboration, the importance is paramount. Google invests billions of dollars in technology, people, and process to ensure data in Google Apps is safe, secure, and private. Google's dedicated team of security professionals is responsible for designing in security from the onset, reviewing all design, code, and finished product to ensure it meets strict Google security and data privacy standards. The same infrastructure used to host Google Apps and secure hundreds of thousands of user's data is also used to manage millions of consumers' data and billions of dollars in advertising transactions. With Google Apps, information is safe and secure.

Google

Introduction

As part of the mission to organize the world's information, Google is responsible for the safekeeping of data for tens of millions of users. This responsibility is taken very seriously, and Google has gone to great lengths to earn and live up to the trust of its users. Google recognizes that secure products are instrumental in maintaining user trust and strives to create innovative products that serve users' needs and operate in their best interest.

Google Apps benefits from this extensive operational experience in producing secure and reliable products. Google's products and services combine advanced technology solutions with industry-leading security practices to ensure customer and user data is secure. Billions of dollars in capital are invested to ensure the most secure, reliable environment for data and applications. In particular, Google focuses on several aspects of security that are critical to business customers:

- Organizational and Operational Security – Policies and procedures to ensure security at every phase of design, deployment and ongoing operations.
- Data Security – Ensuring customer data is stored in secure facilities, on secure servers, and within secure applications.
- Threat Evasion – Protecting users and their information from malicious attacks and would-be hackers.
- Safe Access – Ensuring that only authorized users can access data, and the access channel is secure.
- Data Privacy – Ensuring that confidential information is kept private and confidential

This paper looks at Google's security strategy, which utilizes numerous physical, logical, and operational security measures to ensure the utmost in data security and privacy.

Organizational & Operational Security

The foundation of Google's security strategy starts with its people and processes. Security is a combination of people, processes, and technology, that when put together properly lead to safe and responsible computing. Security is not something that can simply be validated after the fact. Rather, it is designed into products, architecture, infrastructure, and systems from the onset. Google employs a full time security team to develop, document, and implement comprehensive security policies. Google's Security team is made up of some of the world's foremost experts in information, application and network security.

The security team is divided by functional area into perimeter defense, infrastructure defense, application defense, and vulnerability detection and response. Many come to Google with experience in senior information security roles at Fortune 500 companies. This team focuses a large amount of their effort on preventative measures to ensure that code and systems are secure from the onset, and is on call to dynamically respond to security issues

Development Methodology
Google's security posture is top of mind from the moment a product design is drafted. Google engineering and product teams receive extensive training in security fundamentals. Google's development methodology lays out a multi-step plan with ongoing checkpoints and full audits.

The Google Application Security team is involved in all stages of the product development lifecycle including design review, code audit, system and functional testing, and final launch approval. Google uses a number of commercial and proprietary technologies to ensure that applications are secure at every level. Google's Application Security team is also responsible for ensuring that secure development processes are followed to ensure customer safety.

Operational Security
Google's Security Operations team is focused on maintaining security of the operational systems including data handling and system management. These individuals routinely audit datacenter operations and conduct ongoing threat assessment against Google's physical and logical assets.

This group is also responsible for ensuring that all employees are appropriately screened and trained to conduct their job in a professional and secure manner. As appropriate, Google goes to great lengths to screen and verify an individual's background prior to joining the organization. All personnel responsible for maintaining security processes and procedures are thoroughly trained on the practices and continually updated on their training.

Security Community & Advisories
In addition to the processes described above, Google actively works with the security community, leveraging the collective wisdom of the world's best and brightest. This helps Google keep ahead of security trends, quickly react to emerging threats, and harness the expertise of those inside and outside the company. Google actively engages this larger security community through responsible disclosure. Visit **http://www.google.com/corporate/security.html** to find more information about this program and some of the key security experts with whom Google maintains ongoing dialog.

Even with all of these levels of protection, unknown vulnerabilities can emerge, and Google is equipped to respond swiftly to security alerts and vulnerabilities. The Google Security team audits all infrastructure for potential vulnerabilities, and works directly with engineering to correct any known issue immediately. Google Apps Premier Edition customers are notified of user-impacting security issues as soon as practicable via email.

Data Security
The security of company and user data is the mission of Google's Security and Operations teams. Google's business is built on user trust, and therefore this is one of the keys to continued success of Google as a corporation. All Google employees are instilled with the value of responsibility to the end user. Protecting data is at the core of what Google is all about. Google takes great care to protect the billions of dollars of consumer and advertising transactions; we apply that same care to Google's communication and collaboration technologies.

You can see that this is fundamental to who we are as a company by reviewing our code of conduct at **http://investor.google.com/conduct.html**.

Physical Security
Google operates one of the largest networks of distributed datacenters in the world, and goes to great lengths to protect the data and intellectual property in these centers. Google operates datacenters worldwide, and many Google datacenters are wholly owned and managed ensuring that no outside parties can gain access. The geographic locations of the datacenters were chosen to give protection against catastrophic events.. Only select Google employees have access to the datacenter facilities and the servers contained therein, and this access is tightly controlled and audited. Security is monitored and controlled both locally at the site, and centrally at Google's worldwide security operations centers.

The facilities themselves are engineered not only for maximum efficiency, but also for security and reliability. Multiple levels of redundancy ensure ongoing operation and service availability in even the harshest and most extreme of circumstances. This includes multiple levels of redundancy within a center, generator-powered backup for ongoing operations, and full redundancy across multiple dispersed centers. State of the art controls are used to monitor the centers both locally and remotely, and automated failover systems are present to safeguard systems.

Logical Security
In web-based computing, the logical security of data and applications is as critical as physical security. Google goes to extremes to ensure that applications are secure, that data is handled in a secure and responsible way, and that no external unauthorized access to customer or user data can be achieved. To achieve this goal, Google uses a number of industry standard techniques as well as some unique, innovative approaches. One such approach is leveraging special purpose technology as opposed to general-purpose software.

Much of Google's technology is written to provide special purpose capabilities as opposed to general purpose computing. For example, the web server layer is specially designed and implemented by Google to only expose the capabilities required for operation of specific applications. Therefore, it is not as vulnerable to the wide range attacks that most commercial software would be susceptible to.

Google has also made modifications to core libraries for security purposes. Because the Google infrastructure is a dedicated application system rather than a general purpose computing platform, a number of the services provided by the standard Linux operating system can be limited or disabled. These modifications focus on enhancing the capabilities of the system needed for the task at hand and disabling or removing any exploitable aspects of the system that aren't required.

Google's servers are also protected by multiple levels of firewalls to protect against attacks. Traffic is inspected as appropriate for attempted attacks, and any attempts are dealt with to protect users' data.

Information Accessibility
Data such as email is stored in an encoded format optimized for performance, rather than stored in a traditional file system or database manner. Data is dispersed across a number of physical and logical volumes for redundancy and expedient access, thereby obfuscating it from tampering. Google's physical protections described above ensure that no physical access to servers is possible. All access to production systems is conducted by personnel using encrypted SSH (secure shell). Specialized knowledge of the data structures and Google's proprietary infrastructure would be required to get meaningful access to end user data. This is one of many security layers to ensure security of sensitive data within Google Apps.

Google's distributed architecture is built to provide a higher level of security and reliability than a traditional single-tenant architecture. Individual user data is dispersed across a number of anonymous servers, clusters, and datacenters. This ensures that data is not only safe from potential loss, but also highly secure.

User data is only accessible with appropriate credentials, ensuring that there is no possibility of one customer having access to another customer's data without explicit knowledge of their login information. Not only does this proven system serve tens of millions of consumer users with email, calendaring, and documents on a daily basis, but is also used by Google as the primary platform to serve its 10,000+ employee base.

Redundancy
The application and network architecture run by Google is designed for maximum reliability and uptime. Google's grid-based computing platform assumes ongoing hardware failure, and robust software failover withstands this disruption. All Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation.

Data is replicated multiple times across Google's clustered active servers, so, in the case of a machine failure, data will still be accessible through another system. In addition, user data is replicated across datacenters. As a result, if an entire datacenter were to fail or be involved in a disaster, a second datacenter would be able to immediately take over and provide services to users.

Threat Evasion
Email viruses, phishing attacks, and spam are amongst the biggest security threats within corporations today. Reports show that more than two-thirds of incoming mail is spam, new email viruses are born and distributed throughout the Internet each day. Keeping on top of this can be an overwhelming task, and even corporations with spam and virus filters struggle with keeping these constantly up to date to deal with the latest threats. In addition, network-based applications are the target of malicious attacks attempting to tamper with data or bring down the service. Google's world-class threat evasion protects users from attacks on the data and within the content of their messages and files.

Spam and Virus Protection
Google Apps customers benefit from one of the strongest spam and phishing filters in the industry today. Google has developed advanced technology filters that learn from patterns in messages identified as spam, and these filters are trained continually across billions of mail messages. As a result, Google can very accurately identify spam, phishing attacks, and viruses, and ensure sure that users' inboxes, calendars, and documents are protected.

Through Google's web-based interface, virus protection blocks the threat of unknowing users spreading a virus through the corporation or internal network. Unlike traditional client-based email applications, messages are not downloaded to the desktop. Rather, they are scanned on the server for viruses and Gmail will not allow a user to open an attachment until it has been scanned and any threat mitigated. As a result, email viruses cannot take advantage of client-side security vulnerabilities, and users cannot unknowingly open a document with a virus.

Application & Network Attacks
In addition to filtering the content of data for spam and viruses, Google is continuously protecting itself and customers against malicious attacks. Hackers are always looking for ways to pry into web-based applications or bring them down. Denial of service, IP spoofing, cross site scripting, and packet tampering are just a few of the types of attacks that are used against networks daily. Google, being one of the world's largest providers

of web-based services has gone to great lengths to protect against these and other threats. All software is scanned using a variety of commercial and proprietary network and application scanning packages. The Google Security team also works with external parties to test and enhance Google's infrastructure and application security posture.

Safe Access

No matter how secure data is within a datacenter, this data is vulnerable once it's downloaded to a user's local computer. Studies have shown that the average laptop has over 10,000 files and thousands of downloaded email messages. Imagine if one of these corporate laptops falls into the hands of a malicious user. Simply by mounting a disk, an unauthorized user can get access to your corporation's intellectual property and secrets. Google Apps allows companies to mitigate this risk by avoiding the local storage of data onto users' laptops.

End User Protections

The web-based design of Google Apps allows you to make sure that users have ready access to their data from anywhere while the data remains safely on Google's servers. Rather than emails being stored on a desktop or laptop, users have desktop-quality, highly interactive interfaces for email, calendars, and instant messaging while still using a web browser.

Similarly, applications such as Google Docs and Spreadsheets afford users a high level of control over information. These documents stay on the server, but users get rich editing capabilities through the web browser. In addition, users have fine-grained control over who has access to these documents, and can set up a list of editors and viewers. These permissions get enforced on any access to the document, allowing you to avoid the problem of an internal document getting forwarded by email outside your corporation. Finally, these products track changes at a fine-grained level, giving visibility into who made what changes at what time.

Google Apps also protects the transmission of data on the wire, to ensure users are accessing data securely without threat of confidential data being intercepted on the network. Access to the web-based administrative console to Google Apps as well as most end-user applications is offered through a Secure Socket Layer (SSL) connection. Google offers HTTPS access to most services within Google Apps, and the product can be set up to allow only HTTPS access to key services such as email and calendar. With this functionality, all user access to the data and all interactions are encrypted.

At no time does Google use cookies to store passwords or customer data on the user system. Cookies are used for session information and user convenience, but at no time is that information sensitive nor can it be used to break into a user's account.

Giving You Control

In addition to providing these protections on company and user data, Google gives businesses the control to integrate corporate security, access, auditing, and authentication methodologies into Google Apps. Google Apps provides a single sign-on API based on SAML 2.0 which lets companies use existing authentication mechanisms to let users access Google Apps. Businesses can, for example, use Active Directory authentication to log in a user, and the credentials are not transmitted through Google servers for access to the web-based tools. This also allows companies to continue to enforce their password strength and change frequency policies.

In addition, Google provides an administration console and API for user management. Administrators have the power to instantly shut off access to an account or delete an account on demand. This can also be tied to your internal processes for provisioning and deprovisioning a user through the API.

With respect to email and instant messaging, Google also provides the facility to place a mail gateway in front of the mail system. In this configuration, all incoming and outgoing mail goes through the customers system, and this gives you the ability to audit and archive mail, as well as put supervisory controls in place.

Data Privacy

Google is very sensitive to company and user privacy, and realizes that the data housed within applications is confidential and sensitive. Google ensures with Google Apps that information is not compromised. Google's legally binding privacy policy that protects all services can be found by visiting **http://www.google.com/privacypolicy.html**. Per this policy and related policies for the individual services contained within Google Apps, at no time will Google employees access confidential user data. Google also ensures that this policy will not be altered in any potentially damaging way without express written consent from the customer and/or user.

Conclusion

Google Apps provides a secure and reliable platform for your data, bringing you the latest technologies and best practices for datacenter management, network application security, and data integrity. When you entrust your company's information with Google, you can do so with confidence, knowing that the full weight of Google's technology and infrastructure investment is brought to bear to ensure the security, privacy, and integrity of your data.

For more information about Google Apps, go to **http://www.google.com/a** or email **apps-enterprise@google.com**.