1-4024R

Google Apps for Education Agreement

This Google Apps for Education Agreement (the "Agreement") is entered into by and between Google Inc. ("Google"), with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043 and Memorial University of Newfoundland, with an address at Memorial University of Newfoundland, St. John's, NL, Canada, A1C 5S7 P.O. Box 4200 ("Customer"). This Agreement governs Customer's access to and use of the Services and will be effective as of the Effective Date.

1. Services.

1.1 General. Google will provide the Services to Customer during the Term.

1.2 Facilities and Data Transfer. All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data. As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.

1.3 Modifications.

(a) To the Services. Google may make commercially reasonable changes to the Services from time to time. If Google makes a material change to the Services, Google will inform Customer, provided that Customer has subscribed with Google to be informed about such material change.

(b) To URL Terms. Google may make commercially reasonable changes to the URL Terms from time to time. If Google makes a material change to the URL Terms, Google will inform Customer by either sending an email to the Notification Email Address or alerting Customer via the Admin Console. If the change has a material adverse impact on Customer and Customer does not agree to the change, Customer must so notify Google via the Help Center within thirty days after receiving notice of the change. If Customer notifies Google as required, then Customer will remain governed by the terms in effect immediately prior to the change until the end of the then-current Term. If the Services are renewed, they will be renewed under Google's then current URL Terms.

1.4 Aliases. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.

1.5 Ads.

(a) Default. The default setting for the Services is one that does not allow Google to serve Ads. Customer may change this setting in the Admin Console, which constitutes Customer's authorization for Google to serve Ads. If Customer enables the serving of Ads, it may revert to the default setting at any time and Google will cease serving Ads.

(b) Selectively Showing Ads. Notwithstanding Section 1.5(a), if Customer separates different classifications of End Users by domain or Google provides the capability for Customer to show Ads only to particular sets of End Users within the same domain, then Customer must enable the serving of Ads to End Users who are alumni.

1.6 End User Accounts. Customer may request End User Accounts by: (i) requesting them online via the Admin Console; or (ii) after the Services Commencement Date, contacting Google support personnel. Customer can suspend or delete End User Accounts at any point in time through the Admin Console.

2. Customer Obligations.

2.1 Permitted Uses. The Services are permitted for use only by (a) non-profit educational institutions and (b) other non-profit entities (as defined under the relevant state statutes) with 3,000 or less End User Accounts.

2.2 Compliance. Customer will use the Services in accordance with the Acceptable Use Policy. Google may make new applications, features or functionality for the Services available from time to time, the use of which may be contingent upon Customer's agreement to additional terms. In addition, Google will make other Non-Google Apps Products (beyond the Services) available to Customer and its End Users in accordance with the Non-Google Apps Product Terms and the applicable product-specific Google terms of service. If Customer does not desire to enable any of the Non-Google Apps Products, Customer can enable or disable them at any time through the Admin Console.

2.3 Customer Administration of the Services. Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer is responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Agreement. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer and that Google is merely a data-processor.

2.4 End User Consent. Customer's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer's access, monitoring, use and disclosure of this data and Google providing Customer with the ability to do so and (ii) Google to provide the Services.

2.5 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Services and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of, or access to, the Services of which it becomes aware.

2.6 Restrictions on Use. Unless Google specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Services to a third party (unless expressly authorized in this Agreement); (b) attempt to reverse engineer the Services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Services; (d) use the Services for High Risk Activities; or (e) use the Services to store or transfer any Customer Data that is controlled for export under Export Control Laws. Customer is solely responsible for any applicable compliance with HIPAA.

2.7 Third Party Requests. Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information.

3. Technical Support Services.

3.1 By Customer. Customer will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customer's or End Users' use of the Services. Customer will use commercially reasonable efforts to resolve support issues before escalating them to Google.

3.2 By Google. If Customer cannot resolve a support issue consistent with the above, then Customer may escalate the issue to Google in accordance with the TSS Guidelines. Google will provide TSS to Customer in accordance with the TSS Guidelines.

4. Suspension.

4.1 Of End User Accounts by Google. If Google becomes aware of an End User's violation of the Agreement, then Google may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Google's request to Suspend an End User Account, then Google may do so. The duration of any Suspension by Google will be until the applicable End User has cured the breach, which caused the Suspension.

4.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Google may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Google Suspends an End User Account for any reason without prior notice to Customer, at Customer's request, Google will provide Customer the reason for the Suspension as soon as is reasonably possible.

5. Confidential Information.

5.1 Obligations. Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates, employees and agents in violation of this Section.

5.2 Exceptions. Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

5.3 Required Disclosure. Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

5.4 FERPA. The parties acknowledge that (a) Customer Data may include personally identifiable information from education records that are subject to FERPA ("FERPA Records"); and (b) to the extent that Customer Data includes FERPA Records, Google will be considered a "School Official" (as that term is used in FERPA and its implementing regulations) and will comply with FERPA.

6. Intellectual Property Rights; Brand Features.

6.1 Intellectual Property Rights. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.

6.2 Display of Brand Features. Google may display those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Services) within designated areas of the Services Pages. Customer may specify the nature of this use using the Admin Console. Google may also display Google Brand Features on the Services Pages to indicate that Google provides the Services. Neither party may display or use the other party's Brand Features beyond what is allowed in this Agreement without the other party's prior written consent.

6.3 Brand Features Limitation. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features. A party may revoke the other party's right to use its Brand Features pursuant to this Agreement with written notice to the other and a reasonable period to stop the use.

7. Publicity. Neither party may make any public statement regarding the relationship contemplated by this Agreement without the other party's prior written consent. Notwithstanding the foregoing, (a) Customer is permitted to state publicly that it is a customer of the Services, consistent with the Trademark Guidelines, and (b) Customer consents to Google's use of Customer's name in a general customer list, but only if Customer is not the only Customer appearing on the list. For clarification, Customer does not need to seek approval from Google if Customer is repeating a public statement that is substantially similar to a public statement that has been previously approved by Google in accordance with the provisions of this Agreement.

8. Representations, Warranties and Disclaimers.

8.1 Representations and Warranties. Each party represents that it has full power and authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law). Google warrants that it will provide the Services in accordance with the applicable SLA. Customer acknowledges and agrees that it is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998, including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users.

8.2 Disclaimers. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICES. CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS. THE SERVICES ARE NEITHER DESIGNED NOR INTENDED FOR HIGH RISK ACTIVITIES.

9. Term; No Fees.

9.1 Term. This Agreement will remain in effect for the Term.

9.2 Auto Renewal. At the end of the Initial Term and each renewal term, the Services will automatically renew for an additional term of twelve months. If either party does not want the Services to renew, then it must notify the other party in writing at least 15 days prior to the end of the then current term. This notice of non-renewal will be effective upon the conclusion of the then current term.

9.3 No Fees. During the Initial Term, Google will not charge Customer fees for the Services. Upon the parties' mutual written agreement, (a) Google may charge Customer fees for the Services after the Initial Term and (b) Google may

charge Customer fees for a premium version of the Services or for optional functionality or enhancements that may be added to the Services by Google.

9.4 Services Use. Customer has no obligation to use the Services and may cease using the Services at any time for any reason (or no reason).

10. Termination.

10.1 Termination for Breach. Either party may suspend performance or terminate this Agreement if: (i) the other party is in material breach of the Agreement and fails to cure that breach within thirty days after receipt of written notice; (ii) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) the other party is in material breach of this Agreement more than two times notwithstanding any cure of such breaches.

10.2 Other Termination. Customer may terminate this Agreement for any reason (or no reason) with thirty days prior written notice to Google.

10.3 Effects of Termination. If this Agreement terminates, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in this Section); (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates, if applicable, for the Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active servers and overwriting it over time; and (iv) upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party.

11. Indemnification.

11.1 By Google. Google will indemnify, defend, and hold harmless Customer from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim that Google's technology used to provide the Services or any Google Brand Feature infringe or misappropriate any patent, copyright, trade secret or trademark of such third party. Notwithstanding the foregoing, in no event shall Google have any obligations or liability under this Section arising from: (i) use of the Services or Google Brand Features in a modified form or in combination with materials not furnished by Google, and (ii) any content, information or data provided by Customer, End Users or other third parties.

11.2 Possible Infringement.

(a) Repair, Replace, or Modify. If Google reasonably believes the Services infringe a third party's Intellectual Property Rights, then Google will: (a) obtain the right for Customer, at Google's expense, to continue using the Services; (b) provide a non-infringing functionally equivalent replacement; or (c) modify the Services so that they no longer infringe.

(b) Suspension or Termination. If Google does not believe the foregoing options are commercially reasonable, then Google may suspend or terminate Customer's use of the Services with a minimum of six months written notice to Customer, unless prohibited by a court of competent jurisdiction.

11.3 General. Customer will promptly notify Google of the claim and cooperate with Google in defending the claim. Google has full control and authority over the defense, except that: (a) any settlement requiring Customer to admit liability or to pay any money will require Customer's prior written consent, such consent not to be unreasonably withheld or delayed; and (b) Customer may join in the defense with its own counsel at its own expense. THE INDEMNITY ABOVE IS CUSTOMER'S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY GOOGLE OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

12. Limitation of Liability.

12.1 Limitation on Indirect Liability. NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

12.2 Limitation on Amount of Liability. NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN ONE THOUSAND DOLLARS.

12.3 Exceptions to Limitations. These limitations of liability apply to the fullest extent permitted by applicable law, but do not apply to breaches of confidentiality obligations, violations of a party's Intellectual Property Rights by the other party, or indemnification obligations.

13. Miscellaneous.

13.1 Notices. Unless specified otherwise herein: (a) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact; and (b) notice will be deemed given: (i) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified by automated receipt or electronic logs if sent by facsimile or email.

13.2 Assignment. Neither party may assign or transfer any part of this Agreement without the written consent of the other party, except to an Affiliate, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement; and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

13.3 Change of Control. Upon a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction): (a) the party experiencing the change of control will provide written notice to the other party within thirty days after the change of control; and (b) the other party may immediately terminate this Agreement any time between the change of control and thirty days after it receives the written notice in subsection (a).

13.4 Force Majeure. Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.

13.5 No Waiver. Failure to enforce any provision of this Agreement will not constitute a waiver.

13.6 Severability. If any provision of this Agreement is found unenforceable, the balance of the Agreement will remain in full force and effect.

13.7 No Agency. The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

13.8 No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.

13.9 Equitable Relief. Nothing in this Agreement will limit either party's ability to seek equitable relief.

13.10 Governing Law.

a. For State and City Government Entities. If Customer is a city or state government entity, then the parties agree to remain silent regarding governing law and venue.

b. For All other Entities. If Customer is any entity not set forth in Section 13.10(a) then the following applies: This Agreement is governed by New York law, excluding that state's choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN NEW YORK COUNTY, NEW YORK.

13.11 Amendments. Any amendment must be in writing and expressly state that it is amending this Agreement.

13.12 Survival. The following Sections will survive expiration or termination of this Agreement: 5 (Confidential Information), 6.1 (Intellectual Property Rights), 10.3 (Effects of Termination), 11 (Indemnification), 12 (Limitation of Liability), 13 (Miscellaneous) and 15 (Definitions).

13.13 Entire Agreement. This Agreement, and all documents referenced herein, is the parties' entire agreement relating to its subject and supersedes any prior or contemporaneous agreements on that subject. If Customer is presented with a similar agreement on the same subject matter upon its log in to use the Services, this Agreement supersedes and replaces that agreement. The terms located at a URL and referenced in this Agreement are hereby incorporated by this reference.

13.14 Interpretation of Conflicting Terms. If there is a conflict between this Agreement and the URL Terms, this Agreement will control.

13.15 Counterparts. The parties may enter into this Agreement in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

14. Definitions.

"Acceptable Use Policy" means the acceptable use policy for the Services available at http://www.google.com/a/help/intl/en/admins/use_policy.html or such other URL as may be provided by Google.

"Admin Account(s)" means the administrative account(s) provided to Customer by Google for the purpose of administering the Services. The use of the Admin Account(s) requires a password, which Google will provide to Customer.

"Admin Console" means the online tool provided by Google to Customer for use in reporting and certain other administration functions.

"Administrators" mean the Customer-designated technical personnel who administer the Services to End Users on Customer's behalf.

"Ads" means online advertisements displayed by Google to End Users.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party.

"Agreement" means this Google Apps for Education Agreement.

"Brand Features" means the trade names, trademarks, Services marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.

"Confidential Information" means information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is considered Customer's Confidential Information.

"Customer Data" means data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users.

"Customer Domain Names" means the following domain names owned or controlled by Customer, which will be used in connection with the Services: mun.ca. Customer may provide the Services to any of its sub-domains (for example, if Customer Domain Name is "edu.com", a sub-domain may include "alumni.edu.com") without written approval from Google.

"Effective Date" means the date this Agreement is countersigned.

"Emergency Security Issue" means either: (a) Customer's use of the Services in violation of the Acceptable Use Policy, which could disrupt: (i) the Services; (ii) other customers' use of the Services; or (iii) the Google network or servers used to provide the Services; or (b) unauthorized third party access to the Services.

"End Users" means the individuals Customer permits to use the Services.

"End User Account" means a Google-hosted account established by Customer through the Services for an End User.

"Export Control Laws" means all applicable export and re-export control laws and regulations, including the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State.

"FERPA" means the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

"Help Center" means the Google help center accessible at http://www.google.com/support/, or other such URL as Google may provide.

"High Risk Activities" means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as may be amended from time to time, and any regulations issued thereunder.

"Intellectual Property Rights" means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

"Initial Term" means the term that begins on the Effective Date and continues for 5 years.

"Non-Google Apps Products" means Google products which are not part of the Services, but which may be accessed by End Users using their End User Account login and password. The Non-Google Apps Products are set forth at the following URL: http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865, or such other URL as Google may provide.

"Non-Google Apps Product Terms" means the terms found at the following URL: http://www.google.com/apps/intl/en/terms/additional_services.html, or such other URL as Google may provide from time to time.

"Notification Email Address" means the email address designated by Customer to receive email notifications from Google. Customer may change this email address through the Admin Console.

"Services" means the Google Apps for Education Services provided by Google and used by Customer under this Agreement. The Services are described here: http://www.google.com/a/help/intl/en/users/user_features.html, or such other URL as Google may provide.

"Services Commencement Date" is the date upon which Google makes the Services available to Customer.

"Services Pages" mean the web pages displaying the Services to End Users.

"SLA" means the Services Level Agreement located here: http://www.google.com/a/help/intl/en/admins/sla.html, or other such URL as Google may provide.

"Suspend" means the immediate disabling of access to the Services, or components of the Services, as applicable, to prevent further use of the Services.

"Term" means the term of this Agreement, which begins on the Effective Date and continues until the earlier of: (a) the end of the applicable term for the Services or (b) the Agreement is terminated as set forth herein.

"Trademark Guidelines" means Google's Guidelines for Third Party Use of Google Brand Features, located at the following URL: http://www.google.com/permissions/guidelines.html, or other such URL as Google may provide.

"Third Party Request" means a request from a third party for records relating to an End User's use of the Services. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

"TSS" means the technical support services provided by Google to the Administrators during the Term pursuant to the TSS Guidelines.

"TSS Guidelines" means Google's technical support services guidelines then in effect for the Services. TSS Guidelines are at the following URL: http://www.google.com/a/help/intl/en/admins/tssg.html or such other URL as Google may provide.

"URL Terms" means the Acceptable Use Policy, the SLA, and the TSS Guidelines.

IN WITNESS WHEREOF, the parties have executed this Agreement by persons duly authorized as of the Effective Date.

Google		Customer
By:		By: (Authorized Signature)
		Kent Declue (Print Name)
Title:	President, Global Sales and Business Development Google Inc.	Title: VP - Admin & Finance
Date	2012.01.12 16:59:23 -08'00'	Date: 20/12/2011

Addendum

This Addendum (the "Addendum") is incorporated by reference into the Google Apps Enterprise Agreement, Google Apps for Education Agreement, Google Apps for Government Agreement, Google Apps for Business via Reseller Agreement, Google Apps for Government via Reseller Agreement, or Google Apps Enterprise via Reseller Agreement attached to this Addendum between Google and the Customer (as applicable, the "Agreement"). The provisions of this Addendum shall amend or supplement the referenced section(s) of the Agreement as indicated below.

WHEREAS, the parties desire to modify certain provision(s) of the Agreement;

NOW, THEREFORE, for good and valuable consideration, the parties hereto agree as follows:

1. Security Breach Notification. The following is added to the Agreement:

   "Security Breach Notification. To the extent a state or federal security breach law applies to a Security Breach, Google will comply with the applicable law. To the extent no such law applies to a Security Breach, Google will notify Customer of a Security Breach, following the discovery or notification of such Security Breach, in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Google will send any applicable notifications regarding a Security Breach to the Notification Email Address. "Security Breach" means an actual disclosure, or reasonable belief that there has been a disclosure, by Google of Customer Data to any unauthorized person or entity."

2. Security Standards. The following is added to the Agreement:

   "Security Standards. As of the Effective Date, Google abides by the security standards set forth on Exhibit A attached to this Addendum ("Security Standards"). During the Term of the Agreement, the Security Standards may change but Google agrees that any such change shall not cause a material degradation in the security of the Services."

3. Miscellaneous. All other terms and conditions of the Agreement shall remain unchanged and in full force and effect. In the event of a conflict between the terms and conditions of the Agreement and the terms and conditions of this Addendum, the terms and conditions of this Addendum shall govern.

Exhibit A

Security Standards

Google Enterprise Products Security Standards.

1. Personnel. Google has, and will maintain, a security policy for its security personnel, and requires security training as part of the training package for Google security personnel. Google's security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of Google products and services, and for responding to security incidents.

2. Data Storage and Handling. Google will maintain all data on Google-owned servers and disks. Google will replicate data across multiple systems, and will store all decommissioned disks in a secure facility until wiped or destroyed.

3. Data Transmission. Google will transfer all data via internet standard protocols. Gmail, Calendar, Docs and Spreadsheet, and Google Talk offer Customer the ability to encrypt data during transmission using SSL and TLS.

4. Business Continuity Planning/Disaster Recovery. Google will replicate data across multiple separate systems to enhance business continuity in the event of disaster and system failure. Google will maintain a data center infrastructure that is geographically distributed to enhance system redundancy. Google will also maintain a geographically distributed staff to augment system availability in the event of a disaster.

5. Incident Response. Google will monitor a variety of communication channels for security incidents, and Google's security team will react promptly to known incidents.

6. Computer Room Access. Google will store all production data in physically secure datacenters. Google will restrict access to the datacenters on a need-to-know basis to authorized staff.

7. Data and Application Security. Google will logically separate data from different End Users from each other, and only data for an authenticated End User will be displayed to that End User. A central authentication facility is used across all applications to increase uniform security of data.

8. Data Isolation and Architecture. Google will store data in a multi-tenant environment on Google servers. Google will logically isolate data on a per End User basis at the application layer. Google will also logically isolate data on a per organization basis, and each organization will be given control over specific data sharing policies.

9. Change Management. Google will continue to employ a code review process to increase the security of the code used to provide the Services. Google will also continue to employ a security review process to enhance the security products in production environments.

10. Server Operating Systems. Google servers will use a hardened Linux implementation customized for the Google application environment. Google data is stored using Google proprietary algorithms to augment data security and redundancy.

11. Access Control and Privilege Management. Google employs a centralized access management system to control personnel access to Google production servers, and will only provide access to a limited number of authorized personnel. Customers or End Users must authenticate themselves via a central authentication system or via a Customer's single sign on system in order to use the Services. Each application checks credentials in order to allow the display of authorized data to that End User

12. User Accounts. Customer will have control over the creation, deletion, and suspension of End User accounts on Google infrastructure.

13. Password Policy. Customers can use their own password and authentication policy in conjunction with Service using the Google single sign on functionality.

14. Network Connectivity Security Requirements. Google will protect its infrastructure with multiple levels of network devices at multiple layers.

15. SSAE 16. Google has obtained a Standards for Attestation Engagements No. 16 Type II audit report.

16. Data Center Environment and Physical Security. The following is a general description of Google's various data center environments and efforts to ensure physical security in these environments.

    a. Google Data Center Infrastructure. Google maintains a vast number of geographically distributed data centers located primarily in the USA and the European Union.

    b. Physical Security Staffing. Each Google data center maintains a security organization responsible for all data center security functions 24 hours a day, 7 days a week. The security organization monitors Closed Circuit TV (CCTV) cameras and all alarm systems. Internal and external patrols of the data center are performed regularly. The data centers are housed in facilities that require electronic key access, with alarms that are linked to guard stations.

    c. Physical Security Access Procedures. Formal access procedures exist for allowing physical access to the data centers. All entrants to the data center are required to identify themselves as well as show proof of identity to security operations. Valid proof of identity is a photo identification issued by Google and a governmental entity. Only authorized Google employees and contractors are allowed entry to the data centers. Data center managers must approve any visitors in advance for the specific data center and internal areas they wish to visit. Only authorized Google employees and contractors who permanently work at the data centers are permitted to request card access to these facilities. Data center card access requests must be made through e-mail, and requires the approval of the requestor's manager and the data

center director. All other Google employees and authorized contractors requiring temporary data center access must sign in at the guard station, present a Google badge (Google employees or contractors) or ID issued by their employer (authorized contractors) and reference an approved data center access record identifying the individual as approved.

d. Physical Security Devices. Data centers employ electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's access to perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. All entrants to the data centers must pass through a mantrap. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. The CCTV equipment is connected by secure cables throughout the data centers. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

e. Environmental Safeguards.

i. Redundancy. The data centers are designed with resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks. Infrastructure systems have been designed to eliminate single points of failure. Dual circuits, switches, networks or other necessary devices are utilized to provide this redundancy. Critical facilities infrastructure at the data centers have been designed to be robust, fault tolerant and concurrently maintainable. Preventative and corrective maintenance is designed to be performed without interruption of services. All environmental equipment and facilities have documented preventative maintenance procedures that detail the procedure and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the Google data center equipment is scheduled through a standard change process. Preventative maintenance is performed on all infrastructure systems according to documented procedures.

ii. Power.

a. The data center electrical power systems are designed to be fully redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for every critical infrastructure component in the data center. This redundancy begins with dual utility power feeds, primary and alternate, to parallel utility switchboards sized so that any one can provide power to the entire facility. The output power is routed to supply all building loads including uninterruptible power supplies (UPS), building and mechanical services, and heating, ventilation and air conditioning systems.

b. Backup power is provided by various mechanisms including, but not limited to UPS batteries. Backup power is designed to supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted for any reason, backup power is designed to provide transitory power until the diesel generator systems take over. In the event of unavailability of both electrical utility and diesel generators, backup power can provide emergency electrical power to run the data center at full capacity for up to 10 minutes.

c. Diesel engine generators are in place to provide power to critical equipment and customer loads. The generators are capable of providing enough emergency electrical power to run the data center at full capacity typically for a period of days. These generators automatically startup and are able to provide power within seconds in the event of a power outage.

17. Firewalls and Intrusion Detection.

a. Google employs multiple layers of network devices and intrusion detection to ensure that that our external attack surface is protected.

b. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Many companies make extensive use of third-party technologies (e.g., Network Intrusion Detection Systems - NIDS, Host-based Intrusion Detection Systems - HIDS) to look for known attacks against commonly-installed software, and Security Operations Centers (SOCs) to respond when they arise. We take a different approach by:

i. Tightly controlling the size and make-up of our attack surface through preventative measures;
ii. Employing intelligent detect controls at data entry points; and
iii. Employing technologies that automatically remedy dangerous situations.

c. Most of our Internet-exposed attack surface is comprised of Google-created software and the environment involves a large number of servers. Traditional IDS products are not economical, efficient or useful in these situations and we rely on smarter methods of detecting exploitation.

d. When we approach intrusion detection concepts, we break down our attack surface according to anticipated input vectors (i.e., how hackers will attempt to break in). Google's hosting infrastructure is custom-built so we have the ability to tightly define our perimeter and the entrance points into our network. Some of the major areas of coverage that achieve the goals above are as follows:
i. As mentioned previously, the OS on every system is stripped down, modified, and hardened to minimize third party vulnerabilities on running systems;
ii. All IP traffic is routed through custom front end servers that detect and stop malicious requests;

iii. Traffic is examined for exploitation of programming errors via methods such as cross-site scripting, and high priority alerts are generated when such an exploit is found;
iv. To prevent buffer overflow attacks, all open source software that is Internet facing or that processes external data goes through several levels of code review, audit, and modification before allowed into production. All changes are contributed back to the open source community.
v. Systems are checked continually for binary modifications, and any unrecognized modifications are purged;
vi. Router ACLs are used to provide perimeter defense, and an internally routable IP space is used to make sure external connections are never made to internal systems;
vii. Layer 3 filtering is used to mitigate packet-level attacks.

18. Internal Data Access Processes and Policies – Access Policy. LDAP, Kerberos and a Google proprietary system utilizing RSA keys provides Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, customer information and configuration information. We require the use of unique user IDs, strong passwords, and carefully monitored access lists to minimize the potential for inappropriate usage of accounts. The granting or modification of access rights is based on a user's job responsibilities on a need to know basis and must be approved by data owners. Approvals are managed by workflow tools that maintain audit records of all changes. Furthermore, it is Google's policy to provide system access to individuals who have been trained and require this level of access to perform authorized tasks. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication at Google (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., Credit Card data), Google uses hardware tokens.

19. Data Replication, Disaster Recovery, and Data Disposal.

a. Data Replication. Data redundancy is built into all database and file system architectures, and all data that is written to disk is replicated on separate systems. Docs, Spreadsheets and Postini database data is also replicated between multiple data centers to prepare for full data center loss. Such protections help ensure that a customer's data is protected in the event of a disaster. In most cases, customers can also perform their own backups for individual message recovery or archival purposes. Through the mail gateway, a customer can intercept all incoming and outgoing mail, and these can be archived based on any customer criteria. Additionally, each component of the service generally has an API. As a result, an organization can typically pull data out of the service into their own backup whenever needed.

b. Distributed Data Center Architecture. Google does not rely on just one datacenter to run our applications. We operate a geographically distributed set of datacenters to keep services running in the event of incidents and disasters at a single datacenter. All datacenters are connected via high-speed private links to ensure secure and fast data transfer between datacenters. Datacenter locations are undisclosed to the public, and data centers are unmarked to ensure optimal data security. Google's data center management staff is also distributed in multiple geographies to ensure around the clock coverage and system administration that is not location dependent.

c. Deleted data. After an End User confirms deletion of a message, the message in question is immediately deleted from the customer's Google interface and the data is no longer accessible or recoverable by the End User. Pointers to the data on Google's active and replication servers are removed. Dereferenced data will be overwritten with other customer data over time.

d. Media disposal. When retired from Google's systems, every disk containing customer information is subject to a series of data destruction processes before leaving Google's premises. Operational disks are erased in a multi-step process and verified complete by at least two independent validators. The 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, due to hardware failure, the drive cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the disk erase policy.

e. Customer Data Removal from Google Enterprise Products. At any time, an Administrator can delete an End User and their data from Google. Alternatively, an Administrator can suspend an End User or change their password such that their data is accessible to the organization but not the End User. Google provides APIs to most of its Enterprise applications so an Administrator may migrate End Users and data off of Google Enterprise Products at any point. For customer protection, a Google Enterprise product domain can only be cancelled and deleted by calling our support center. The support staff will verify the caller's status as an Administrator and will delete the account. The account can take up to five days to delete within the system.