Addendum n^{o} 1

à l'accord *Google Apps for Education*

Le présent Addendum (l'« **Addendum** ») est incorporé par renvoi à l'Accord *Google Apps for Education* (l'« **Accord** ») conclu entre Google Inc. (« **Google**") et le client nommé dans le bon de commande (le « **client** ») à compter de la date à laquelle le client a cliqué sur le bouton « J'accepte » ou, le cas échéant, de celle à laquelle l'Accord est contresigné (la « **date d'entrée en vigueur** »). Les dispositions du présent Addendum modifient ou complètent l'Accord. En cas de conflit entre les dispositions du présent Addendum et celles de l'Accord, ce sont les dispositions de l'Addendum qui ont préséance.

1. La définition de l'expression « données sur les clients » qui figure dans l'Accord est entièrement remplacée par la suivante :

   « "données sur les clients" Désigne les données, y compris les courriels, que les clients ou les utilisateurs ultimes fournissent, génèrent, transmettent, affichent ou stockent par l'entremise des Services. »

2. La définition de l'expression « renseignements confidentiels » qui figure dans l'Accord est entièrement remplacée par la suivante :

   « "Renseignements confidentiels" Désigne les renseignements désignés comme confidentiels ou normalement considérés comme confidentiels dans les circonstances que l'une des parties communique à l'autre en vertu du présent Accord. Les données sur les clients sont considérées comme des renseignements confidentiels des clients. Les clients ou les utilisateurs ultimes, selon le cas, sont propriétaires de la totalité des données sur les clients. »

3. La section qui suit est ajoutée à l'Accord :

   « a. Reconnaissance de la LAIMPVP "LAIMPVP" Désigne la *Loi sur l'accès à l'information municipale et la protection de la vie privée*, Lois refondues de l'Ontario de 1990, chapitre M.56, dans sa forme modifiée. Le client avise Google qu'il est assujetti à la LAIMPVP. Google s'engage à s'efforcer de manière raisonnable sur le plan commercial de procurer au client un accès opportun aux comptes d'utilisateur ultime et aux données sur les clients, dans les limites fixées à la section 2.7 (ou à la section équivalente intitulée "Demandes d'un tiers"). Il incombe au client d'évaluer si l'utilisation des Services concorde avec les obligations juridiques que lui impose la LAIMPVP.

   b. Indemnisation par le client. Le client s'engage à indemniser Google à l'égard de toute amende liée à une violation de la LAIMPVP. »

4. La section suivante est ajoutée à l'Accord :

   « "Utilisation des données sur les clients" Google utilisera les données sur les clients aux fins suivantes : a) fournir les Services; b) exploiter, tenir à jour,

améliorer et soutenir l'infrastructure servant à fournir les Services, et c) se conformer aux directives des clients ou des utilisateurs ultimes quant à l'utilisation, la gestion et l'administration des Services, d) répondre aux demandes de soutien des clients. Google n'utilisera les données sur les clients que d'une manière conforme au présent Accord. »

5. La phrase suivante est ajoutée à la fin de la section 12.3 (ou de la section équivalente intitulée "Effets de la résiliation") de l'Accord :

   « Si le client supprime des données, Google supprimera ces données et les pointeurs qui y mènent dans les serveurs actifs et les serveurs de réplication. »

6. La section 10.1 (ou la section équivalente intitulée « Déclarations et garanties ») de l'Accord est entièrement remplacée par la suivante :

   « Chaque partie déclare qu'elle a pleins pouvoirs pour conclure l'Accord. Chacune garantit qu'elle se conformera à la totalité des lois et des règlements qui s'appliquent à la prestation ou à l'utilisation des Services. Google garantit qu'elle fournira les Services d'une manière conforme à l'ANS applicable. Le client déclare qu'il est un établissement d'enseignement. L'expression "établissement d'enseignement" désigne n'importe quelle école primaire ou secondaire du secteur public ou n'importe quel conseil scolaire ou programme d'enseignement administré par un conseil scolaire sur tout le territoire de la province de l'Ontario, et, de plus, les écoles autochtones et des Premières Nations de l'Ontario administrées dans le cadre du programme d'enseignement de l'Ontario qui est en vigueur, les facultés d'éducation du secteur public ainsi que les instituts de formation pédagogique de l'Ontario; il est entendu que l'expression "établissement d'enseignement" exclut les écoles privées. Le client reconnaît et convient qu'il est seul chargé de veiller au respect de la *Children's Online Privacy Protection Act of 1998* (États-Unis) et, en particulier, d'obtenir le consentement des parents en vue de recueillir les renseignements confidentiels sur les élèves que les clients et les utilisateurs ultimes utilisent en liaison avec les Services. »

7. La section suivante est ajoutée à l'Accord :

   « À la date d'entrée en vigueur de l'Accord, Google se conforme aux normes de sécurité décrites dans la pièce jointe A ("Normes de sécurité"). Il est possible que ces normes changent pendant la durée de l'Accord, mais Google convient qu'aucun changement de cette nature n'entraînera une détérioration marquée de la sécurité des Services. »

Pièce jointe A

Normes de sécurité relatives à Google Apps

Dans les normes de sécurité exposées ci-après, et à moins d'une indication contraire dans la présente, le mot « services » désigne les programmes suivants : *Google Apps for Business*, *Google Apps for Education*, *Google Apps for Government* et *Google Apps – Postini Services*.

1. Sécurité des centres de données et du réseau

   a. Centres de données

      i. Infrastructure. Google tient un nombre élevé de centres de données géographiquement dispersés qu'elle gère ou qu'elle possède. Google stocke la totalité des données de production dans des centres de données physiquement sûrs.

      ii. Redondance. Les systèmes d'infrastructure sont conçus pour éliminer les points de défaillance uniques et amoindrir l'effet des risques environnementaux anticipés. Des circuits doubles, des commutateurs, des réseaux ou d'autres dispositifs nécessaires aident à assurer cette redondance. Les Services sont conçus pour permettre à Google d'exécuter de façon ininterrompue certaines activités d'entretien préventif et correctif. Toutes les installations et tout le matériel environnemental sont dotés de procédures d'entretien préventif documentées, qui exposent en détail le processus à suivre et la fréquence d'exécution, conformément à des spécifications internes ou à celles du fabricant. L'entretien préventif et correctif du matériel des centres de données est planifié au moyen d'un processus de changement standard qui est conforme aux procédures documentées.

      iii. Alimentation. Les systèmes d'alimentation électrique des centres de données sont conçus pour être redondants et maintenables sans effet sur la continuité des activités, 24 heures sur 24, sept jours sur sept. Dans la plupart des cas, une source d'alimentation principale et une source d'alimentation de secours, offrant chacune une capacité égale, est prévue pour les éléments d'infrastructure critiques que comportent les centres de données. L'alimentation de réserve est assurée par divers mécanismes, comme des blocs d'alimentation sans interruption (ASI), qui protègent l'alimentation de manière constante et fiable lors des restrictions de courant, des pannes de courant, des surtensions, des sous-tensions et des fréquences hors tolérances. S'il survient une panne de courant, l'alimentation de réserve est conçue pour fournir une alimentation de transition aux centres de données, à pleine capacité, pendant une période maximale de dix minutes, jusqu'à ce que les groupes électrogènes diesel prennent le relais. Ces derniers sont capables de se mettre automatiquement en marche en moins de quelques secondes, de façon à assurer une alimentation électrique d'urgence suffisante pour faire fonctionner les centres de données à pleine capacité, habituellement pendant une période de plusieurs jours.

      iv. Systèmes d'exploitation des serveurs. Les serveurs de Google utilisent une version basée sur Linux et adaptée à l'environnement d'application de Google. Les données des clients sont stockées à l'aide d'algorithmes exclusifs à Google, de façon à

améliorer la sécurité des données et la redondance. Google a recours à un processus d'examen de codes qui permet de rehausser la sécurité des codes employés dans le cadre de la fourniture des Services et d'améliorer les produits de sécurité dans les environnements de production.

v. Continuité des activités. Google a conçu et exécute régulièrement des activités de planification et de mise à l'essai de ses programmes de planification de la continuité des activités et/ou de reprise après catastrophe.

b. Réseaux et transmission.

i. Transmission des données. Les centres de données sont habituellement branchés au moyen de liaisons privées à haute vitesse qui permettent de transférer rapidement et sûrement les données entre les divers centres de données. Google transfère la totalité des données sur les clients au moyen de protocoles Internet standards.

ii. Surface d'attaque externe. Google a recours à de multiples couches de dispositifs réseau et de mesures de détection des intrusions en vue de protéger la surface d'attaque externe de Google. Google examine les vecteurs d'attaque potentiels et incorpore des technologies spécialisées appropriées dans ses systèmes à orientation externe.

iii. Détection des intrusions. Les mesures de détection des intrusions visent à fournir des informations sur les activités d'attaque qui sont en cours ainsi qu'à fournir des informations appropriées en vue de réagir à un incident L'approche de Google à cet égard consiste à :

1. contrôler de près la taille et la composition de sa surface d'attaque grâce à des mesures préventives;

2. recourir à des mécanismes de contrôle de détection intelligents aux points d'entrée des données;

3. utiliser des technologies qui corrigent automatiquement certaines situations dangereuses.

iv. Réaction aux incidents. Google surveille diverses voies de communication en vue d'y repérer les incidents relatifs à la sécurité, et son personnel de sécurité réagit rapidement aux incidents connus.

2. Contrôle de l'accès et des sites

a. Contrôle des sites

i. Services de sécurité interne dans les centres de données. Chaque centre de données de Google tient sur place un service de sécurité chargé de toutes les fonctions de sécurité matérielle concernant ce centre de données, et ce, 24 heures sur 24, sept jours sur sept. Le personnel de ce service surveille des caméras de télévision en circuit fermé

(CTCF) ainsi que tous les systèmes d'alarme. Le personnel mène régulièrement des patrouilles internes et externes dans le centre de données.

ii. Procédures d'accès aux centres de données. Google tient des procédures formelles au sujet de l'accès physique aux centres de données. Ces derniers sont situés dans des installations qui exigent un accès par carte électronique, et ils sont dotés d'avertisseurs reliés au Service de sécurité interne. Toutes les personnes qui entrent dans le centre de données sont tenues de s'identifier ainsi que de montrer une preuve d'identité au personnel du Service de sécurité interne. Seuls les employés de Google, les entrepreneurs et les visiteurs autorisés peuvent entrer dans les centres de données. Seuls les employés et les entrepreneurs de Google sont autorisés à demander un accès par carte électronique à ces installations. Les demandes d'accès par carte électronique aux centres de données doivent être présentées par courriel, et être autorisées par le gestionnaire de l'auteur de la demande ainsi que par le directeur du centre de données concerné. Toutes les autres personnes ayant besoin d'un accès temporaire à un centre de données doivent : (i) obtenir à l'avance l'autorisation des gestionnaires du centre de données et des secteurs internes dans lesquels elles souhaitent se rendre, (ii) s'inscrire auprès du Service de sécurité interne et (iii) faire référence à un document d'accès au centre de données autorisé qui indique que la personne en question a été approuvée.

iii. Dispositifs de sécurité présents dans les centres de données. Les centres de données de Google utilisent un système de contrôle par carte électronique et accès biométrique qui est relié à une alarme de système. Le système de contrôle de l'accès surveille et enregistre la carte électronique de chaque personne ainsi que les moments où celle-ci franchit une porte périmétrique ou se rend à la zone d'expédition et de réception ainsi qu'à d'autres zones critiques. Les activités non autorisées et les tentatives d'accès manquées sont enregistrés par le système de contrôle de l'accès et, s'il y a lieu, font l'objet d'une enquête. L'accès autorisé dans tous les secteurs d'activités et les centres de données est limité en fonction des zones et des responsabilités professionnelles de la personne. Les portes coupe-feu des centres de données sont munies d'un avertisseur. Des CTCF fonctionnent tant à l'intérieur qu'à l'extérieur des centres de données. Ces caméras sont disposées de manière à couvrir des zones stratégiques dont, notamment, le périmètre, les portes du bâtiment du centre de données, ainsi que les zones d'expédition et de réception. Le personnel du Service de sécurité interne gère le matériel de surveillance, d'enregistrement et de contrôle du système de télévision en circuit fermé. Ce matériel est relié par des câbles sécuritaires dans tous les centres de données. Les caméras sont reliées à des enregistreurs vidéonumériques et tournent 24 heures sur 24, sept jours sur sept. Les documents de surveillance sont conservés pendant une période pouvant atteindre 90 jours, suivant l'activité en question.

b. Contrôle de l'accès

i. Personnel de sécurité de l'infrastructure. Google a établi et tient à jour une politique de sécurité concernant les membres de son personnel, et elle exige qu'une formation en sécurité fasse partie de la formation générale dispensée aux membres de son

personnel. Le personnel de la sécurité de l'infrastructure de Google est chargé de surveiller de façon permanente l'infrastructure de sécurité de Google, d'examiner les Services ainsi que de réagir aux incidents de sécurité.

ii. Contrôle de l'accès et gestion des privilèges. Les administrateurs et les utilisateurs ultimes sont tenus de s'authentifier au moyen d'un système d'authentification central ou d'un système d'inscription unique des clients en vue de pouvoir utiliser les Services. Chaque demande permet de vérifier les justificatifs d'identité avant d'autoriser l'affichage de données à un utilisateur ultime ou à un administrateur autorisé.

iii. Processus et politiques internes d'accès aux données – Politique d'accès. Google recourt à un système de gestion centralisée de l'accès en vue de limiter l'accès du personnel à ses serveurs de production, et elle n'y donne accès qu'à un nombre restreint de membres du personnel autorisés. LDAP, Kerberos et un système exclusif à Google utilisant un système de clés RSA sont conçus pour fournir à Google des mécanismes d'accès sûrs et souples. Ces derniers sont conçus pour n'accorder que des droits d'accès approuvés aux hébergeurs de sites, aux connexions, aux données sur les clients et aux informations de configuration. Google oblige à utiliser des ID d'utilisateurs uniques, ainsi que des mots de passe forts, un système d'authentification à deux facteurs et des listes d'accès soigneusement surveillées, de façon à réduire le risque d'une utilisation non autorisée des comptes. L'octroi ou la modification des droits d'accès reposent sur les aspects suivants : les responsabilités professionnelles du personnel autorisé, les exigences professionnelles nécessaires pour exécuter les tâches autorisées, le principe de l'accès sélectif, de même que le respect des politiques et des activités de formation internes en matière d'accès aux données de Google. Les autorisations sont gérées par des outils qui assurent la vérification de tous les changements. L'accès aux systèmes est enregistré en vue de créer une piste de vérification à des fins de responsabilisation. Lorsqu'on utilise des mots de passe à des fins d'authentification chez Google (p. ex. : connexion à des postes de travail), ce sont des règles en matière de mots de passe qui respectent à tout le moins les pratiques standards de l'industrie qui sont mises en oeuvre. Ces normes présentent les caractéristiques suivantes : expiration du mot de passe, restrictions au sujet de la réutilisation d'un mot de passe et robustesse suffisante du mot de passe. Pour ce qui est de l'accès aux renseignements extrêmement sensibles (comme les données relatives aux cartes de crédit), Google se sert de jetons matériels.

c. Vérifications et certifications. Pendant la durée de l'entente, Google tiendra à jour son rapport de vérification établi en vertu de la *Standard for Attestation Engagement No. 16* (SSAE 16) ou un rapport comparable (le « rapport de vérification »), ainsi que de sa certification ISO/IEC 27001:2005 ou une certification comparable (la « certification ISO ») pour les services de base de *Google Apps*. Google mettra à jour le rapport de vérification à intervalles d'au moins dix-huit (18) mois.

d. Atteinte à la sécurité. Dans la mesure où une loi étatique ou fédérale en matière d'atteintes à la sécurité s'applique à une atteinte à la sécurité, Google se conformera à cette loi. Dans la mesure où aucune loi de cette nature ne s'applique à une atteinte à la

sécurité, Google avisera le client d'une atteinte à la sécurité à la suite de la découverte ou de la notification de cette dernière, et ce, le plus rapidement possible dans les circonstances, sans délai déraisonnable, conformément au besoin légitime de faire respecter les lois applicables, et après avoir pris toutes les mesures requises pour déterminer l'étendue de l'atteinte et rétablir l'intégrité raisonnable du système. Google transmettra toutes les notifications applicables concernant une atteinte à la sécurité à l'adresse courriel de notification ou communiquera directement avec le client (p. ex., appel téléphonique, rencontre en personne, etc.). Pour les besoins de la présente Section, l'expression « atteinte à la sécurité » désigne une divulgation réelle, ou une croyance raisonnable qu'il y a eu divulgation, par Google, de données sur les clients à une personne ou à une entité non autorisée.

3. Données

a. Stockage, isolement et authentification des données. Google stocke les données des clients dans un environnement à locataires multiples dans des serveurs qui lui appartiennent. Les données sur les clients, la base de données relative aux Services et l'architecture des systèmes de fichiers sont répliqués entre de multiples centres de données dispersés sur le plan géographique. Google isole logiquement les données en fonction des utilisateurs ultimes au niveau de la couche application. Google isole également de manière logique les données en fonction des comptes des clients, et chacun de ces comptes peut exercer un contrôle sur les politiques précises en matière de partage de données. Google sépare logiquement les données des différents utilisateurs ultimes, et les données qui s'appliquent à un utilisateur ultime authentifié ne seront pas affichées à un autre utilisateur ultime (sauf si l'ancien utilisateur ultime ou administrateur en donne l'autorisation). Google utilise un système central d'authentification qui recoupe l'ensemble des Services afin d'uniformiser davantage la sécurité des données.

b. Politique en matière d'effacement et de déclassement des disques. Certains disques contenant des données des clients peuvent présenter des problèmes d'exécution, des erreurs ou des défaillances de matériel qui amènent Google à les déclasser (« disque déclassé »). Chaque disque déclassé est soumis à une série de processus de destruction de données (la « Politique d'effacement des disques ») avant de quitter les installations de Google en vue d'être réutilisé ou détruit. Les disques déclassés sont effacés dans le cadre d'un processus à plusieurs étapes et ils sont vérifiés par au moins deux valideurs indépendants. Les résultats de l'effacement sont enregistrés sous le numéro de série du disque déclassé pour fins de suivi. Enfin, le disque déclassé que l'on a effacé est remis en circulation pour réutilisation et redéploiement. S'il est impossible d'effacer le disque déclassé à cause d'une panne de matériel, ce dernier est stocké en lieu sûr jusqu'à ce qu'il soit possible de le détruire. Chaque installation est vérifiée régulièrement afin de déterminer si elle respecte la Politique d'effacement des disques.