G Suite

Data Processing Amendment to Google Apps Agreement

The Customer agreeing to these terms ("**Customer**") and Google Inc., Google Ireland Limited, Google Commerce Limited or Google Asia Pacific Pte. Ltd. (as applicable, "**Google**") have entered into a Google Apps for Work Agreement, Google Apps Enterprise Agreement, Google Apps for Business Agreement, Google Apps for Work via Reseller Agreement, Google Apps Enterprise via Reseller Agreement, Google Apps for Business via Reseller Agreement, Google Apps for Education Agreement or Google Apps for Education via Reseller Agreement, as applicable (as amended to date, the "**Google Apps Agreement**"). This amendment (the "**Data Processing Amendment**") is entered into by Customer and Google as of the Amendment Effective Date and amends the Google Apps Agreement.

The "**Amendment Effective Date**" is: (a) if this Data Processing Amendment is incorporated into the Google Apps Agreement by reference, the effective date of the Google Apps Agreement, as defined in that agreement; or (b) if this Data Processing Amendment is not incorporated into the Google Apps Agreement by reference, the date Customer accepts this Data Processing Amendment by clicking to accept these terms.

If this Data Processing Amendment is not incorporated into the Google Apps Agreement by reference and you are accepting on behalf of Customer, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms; (ii) you have read and understand these terms; and (iii) you agree, on behalf of the party you represent, to this Data Processing Amendment. If you do not have the legal authority to bind Customer, please do not click the "I Accept" button.

1. **Introduction.**

   This Data Processing Amendment reflects the parties' agreement with respect to terms governing the processing of Customer Data under the Google Apps Agreement.

2. **Definitions.**

   2.1. Capitalized terms used but not defined in this Data Processing Amendment have the meanings given in the Google Apps Agreement. In this Data Processing Amendment, unless expressly stated otherwise:

   "**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

   "**Advertising**" means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any Google Affiliate display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using the "Google Sites" functionality within the Services).

   "**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

   "**Agreement**" means the Google Apps Agreement, as amended by this Data Processing Amendment and as may be further amended from time to time in accordance with the Google Apps Agreement.

   "**Customer Data**" means data (which may include personal data and the categories of data referred to in Appendix 1) submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

"**Data Incident**" means (a) any unlawful access to Customer Data stored in the Services or systems, equipment or facilities of Google or its Sub-processors, or (b) unauthorized access to such Services, systems, equipment or facilities that results in loss, disclosure or alteration of Customer Data.

"**Data Privacy Officer**" means Google's Data Privacy Officer for Apps.

"**Data Protection Legislation**" means, as applicable: (a) any national provisions adopted pursuant to the Directive that are applicable to Customer and/or any Customer Affiliates as the controller(s) of the Customer Data; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

"**EEA**" means the European Economic Area.

"**Google Group**" means those Google Affiliates involved in provision of the Services to Customer.

"**Instructions**" means Customer's written instructions to Google consisting of the Agreement, including instructions to Google to provide the Services and technical support for the Services as set out in the Agreement; instructions given by Customer, its Affiliates and End Users via the Admin Console and otherwise in its and their use of the Services and related technical support services; and any subsequent written instructions given by Customer to Google and acknowledged by Google.

"**Model Contract Clauses**" or "**MCCs**" means the standard contractual clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Safe Harbor Certification**" means a current certification to the U.S. Department of Commerce Safe Harbor framework requirements as set out at the following URL: http://export.gov/safeharbor/eu/eg_main_018475.asp, or any replacement framework or URL from time to time.

"**Services**" means, for purposes of this Data Processing Amendment, the Google Apps for Work Services which are described at www.google.com/apps/intl/en/terms/user_features.html (as such services and URL link may be updated or modified by Google from time to time in accordance with the Google Apps Agreement).

"**Subprocessors**" means (a) all Google Group entities that have logical access to and process Customer Data (each, a "**Google Group Subprocessor**"); and (b) all third parties (other than Google Group entities) that are engaged to provide services to Customer and that have logical access to and process Customer Data (each, a "**Third Party Subprocessor**").

"**Term**" means the term of the Google Apps Agreement, as defined in that agreement.

"**Third Party Auditor**" means a qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

2.2. The terms "personal data", "processing", "data subject", "controller" and "processor" have the meanings given to them in the Directive. The terms "data importer" and "data exporter" have the meanings given to them in the Model Contract Clauses.

3. **Term.**

This Data Processing Amendment will take effect on the Amendment Effective Date and, notwithstanding expiry or termination of the Google Apps Agreement, will remain in effect until, and automatically terminate upon, deletion by Google of all data as described in Section 7 (Data Deletion) of this Data Processing Amendment.

4. **Data Protection Legislation.**

The parties agree and acknowledge that the Data Protection Legislation may apply to the processing of Customer Data.

5. **Processing of Customer Data.**

5.1. **Controller and Processor**. If the Data Protection Legislation applies to the processing of Customer Data, then as between the parties, the parties acknowledge and agree that: (a) Customer is the controller of Customer Data under the Agreement; (b) Google is a processor of such data; (c) Customer will comply with its obligations as a controller under the Data Protection Legislation; and (d) Google will comply with its obligations as a processor under the Agreement. If under the Data Protection Legislation a Customer Affiliate is considered the controller (either alone or jointly with the Customer) with respect to certain Customer Data, Customer represents and warrants to Google that Customer is authorized (i) to give the Instructions to Google and otherwise act on behalf of such Customer Affiliate in relation to such Customer Data as described in this Data Processing Amendment, and (ii) to bind the Customer Affiliate to the terms of this Data Processing Amendment.

5.2. **Scope of Processing**. Google will only process Customer Data in accordance with the Instructions, and will not process Customer Data for any other purpose.

5.3. **Processing Restrictions**. Notwithstanding any other term of the Agreement, Google will not process Customer Data for Advertising purposes or serve Advertising in the Services.

5.4. **Additional Products**. Customer acknowledges that if it installs, uses, or enables Additional Products, the Services may allow such Additional Products to access Customer Data as required for the interoperation of those Additional Products with the Services. This Data Processing Amendment does not apply to the processing of data transmitted to or from such Additional Products. Customer can enable or disable Additional Products. Customer is not required to use Additional Products in order to use the Services.

6. **Data Security; Security Compliance; Audits.**

6.1. **Security Measures**. Google will take and implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss or alteration or unauthorized disclosure or access or other unauthorized processing, as detailed in Appendix 2 ("**Security Measures**"). Google may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. Customer agrees that it is solely responsible for its use of the Services, including securing its account authentication credentials, and that Google has no obligation to protect Customer Data that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (e.g., offline or on-premise storage).

6.2. **Security Compliance by Google Staff**. Google will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance.

6.3. **Data Incidents**. If Google becomes aware of a Data Incident, Google will promptly notify Customer of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by Customer in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring the contact information given for purposes of the Notification Email Address is current and valid, and for fulfilling any third party notification obligations. Customer agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems; or (ii) accidental loss or disclosure of Customer Data caused by Customer's use of the Services or Customer's loss of account authentication credentials. Google's obligation to report or respond to a Data Incident under this Section will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

6.4. **Compliance with Security and Privacy Standards; SOC 2 and 3 Reports**. During the Term, Google will maintain the following:

(a) its ISO/IEC 27001:2013 Certification or a comparable certification ("**ISO 27001 Certification**") for the Services;

(b) conformity of the Services with ISO/IEC 27018:2014 or a comparable standard ("**ISO 27018 Conformity**"), as independently verified;

(c) its confidential Service Organization Control (SOC) 2 Report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability as related to the Services (the "**SOC 2 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months; and

(d) its Service Organization Control (SOC) 3 Report (or a comparable report) as related to the Services (the "**SOC 3 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months.

6.5. **Auditing Security Compliance**

6.5.1. **Reviews of Security Documentation.** Google will make the following available for review by Customer:

(a) the certificate issued in relation to Google's ISO 27001 Certification;

(b) the then-current SOC 3 Report;

(c) a summary or redacted version of the then-current confidential SOC 2 Report; and

(d) following a request by Customer in accordance with Section 6.5.4 below, the then-current confidential SOC 2 Report.

6.5.2. **Customer Audits.** If Customer (or an authorized Customer Affiliate) has entered into Model Contract Clauses as described in Section 10.2 of this Data Processing Amendment, Customer or such Customer Affiliate may exercise the audit rights granted under clauses 5(f) and 12(2) of such Model Contract Clauses:

(a) by instructing Google to execute the audit as described in Sections 6.4 and 6.5.1 above; and/or

(b) following a request by Customer in accordance with Section 6.5.4 below, by executing an audit as described in such Model Contract Clauses.

6.5.3. **Additional Business Terms for Reviews and Audits.** Google and Customer (or an authorized Customer Affiliate if applicable) will discuss and agree in advance on:

(a) the reasonable date(s) of and security and confidentiality controls applicable to any Customer review under Section 6.5.1(d); and

(b) the identity of a suitably qualified and independent third party auditor for any audit under Section 6.5.2(b), and the reasonable start date, scope and duration of and security and confidentiality controls applicable to any such audit.

Google reserves the right to charge a fee (based on Google's reasonable costs) for any review under Section 6.5.1(d) and/or audit under Section 6.5.2(b). For clarity, Google is not responsible for any costs incurred or fees charged by any third party auditor appointed by Customer (or an authorized Customer Affiliate) in connection with an audit under Section 6.5.2(b). Nothing in this Section 6.5 varies or modifies any rights or obligations of Customer (or any authorized Customer Affiliate) or Google Inc. under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA) of this Data Processing Amendment.

6.5.4. **Requests for Reviews and Audits.** Any requests under Section 6.5.1 or 6.5.2 must be sent to the Data Privacy Officer as described in Section 9 (Data Privacy Officer) of this Data Processing Amendment.

7. **Data Deletion.**

7.1. **Deletion by Customer and End Users**. During the Term, Google will provide Customer or End Users with the ability to delete Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Customer or End User deletes Customer Data and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash" ("**Customer-Deleted Data**"), Google will delete such data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

7.2. **Deletion on Standard Termination**. On expiry or termination of the Google Apps Agreement (or, if applicable, on expiry of any post-termination period during which Google may agree to continue providing the Services), Google will, subject to Section 7.3 (Deletion on Termination for Non-Payment or No Purchase) below, delete all Customer-Deleted Data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

7.3. **Deletion on Termination for Non-Payment or No Purchase**. On termination of the Google Apps Agreement due to Customer breaching its payment obligations or opting not to purchase the Services at the end of a free trial of the Services, Google will delete all Customer Data from its systems within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

8. **Access to Data.**

8.1. **Access; Export of Data**. During the Term, Google will provide Customer with access to and the ability to correct, block and export Customer Data in a manner consistent with the functionality of the Services and in

accordance with the terms of the Agreement. To the extent Customer, in its use and administration of the Services during the Term, does not have the ability to correct or block Customer Data as required by applicable law, or to migrate Customer Data to another system or service provider, Google will comply with any reasonable requests by Customer to assist in facilitating such actions to the extent Google is legally permitted to do so and has reasonable access to the Customer Data.

8.2. **End User Requests**. During the Term, if Google receives any request from an End User for records relating to that End User's personal data included in the Customer Data, Google will advise such End User to submit its request to Customer. Customer will be responsible for responding to any such request using the functionality of the Services.

9. **Data Privacy Officer.**

The Data Privacy Officer can be contacted by Customer Administrators at: https://support.google.com/a/contact/gfw_dpo (or via such other means as may be provided by Google). Administrators must be signed in to their Admin Account to use this address.

10. **Data Transfers.**

10.1. **Data Storage and Processing Facilities**. Google may store and process Customer Data in the United States or any other country in which Google or any of its Subprocessors maintains facilities, subject to Section 10.2 (Transfers of Data Out of the EEA) below.

10.2. **Transfers of Data Out of the EEA**. If the storage and processing of Customer Data (as set out in Section 10.1 above) involves transfers of Customer personal data out of the EEA and Data Protection Legislation applies to those transfers, Google will:

10.2.1 ensure that Google Inc. maintains its Safe Harbor Certification, and that the transfers are made in accordance with such Safe Harbor Certification; and/or

10.2.2 ensure that Google Inc. as the data importer of such Customer personal data enters into Model Contract Clauses with Customer (or an authorized Customer Affiliate) as the data exporter of such data, if Customer so requests, and that the transfers are made in accordance with any such Model Contract Clauses; and/or

10.2.3 adopt an alternative solution that achieves compliance with the terms of the Directive for transfers of personal data to a third country, and ensure that the transfers are made in accordance with any such compliance solution.

10.3. **Safe Harbor Certification and Processing Practices**. While Google Inc. maintains its Safe Harbor Certification pursuant to Section 10.2.1, Google will ensure that: (a) the scope of such Safe Harbor Certification includes Customer Data; and (b) the Google Group's processing practices in respect of Customer Data remain consistent with those described in such Safe Harbor Certification.

10.4. **Data Center Information**. Google will make available to Customer information about the countries in which data centers used to store Customer Data are located.

11. **Subprocessors.**

11.1. **Subprocessors**. Google may engage Subprocessors to provide parts of the Services and related technical support services, subject to the restrictions in this Data Processing Amendment.

11.2. **Subprocessing Restrictions**. Google will ensure that Subprocessors only access and use Customer Data in accordance with the terms of the Agreement and that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required by the following, as applicable pursuant to Section 10.2 (Transfers of Data Out of the EEA): (a) any Safe Harbor Certification maintained by Google Inc.; (b) any Model Contract Clauses entered into by Google Inc. and Customer (or an authorized Customer Affiliate); and/or (c) any alternative compliance solution adopted by Google.

11.3. **Consent to Subprocessing**. Customer consents to Google subcontracting the processing of Customer Data to Subprocessors in accordance with the Agreement. If the Model Contract Clauses have been entered into as described above, Customer (or, if applicable, an authorized Customer Affiliate) consents to Google Inc. subcontracting the processing of Customer Data in accordance with the terms of the Model Contract Clauses.

11.4. **Additional Information**. Information about Third Party Subprocessors is available at the following URL: www.google.com/intl/en/work/apps/terms/subprocessors.html, as such URL may be updated by Google from time to time. The information available at the URL is accurate at the time of publication. At the written request of the Customer, Google will provide additional information regarding Subprocessors and their locations. Any such requests must be sent to the Data Privacy Officer for Google Apps as described in Section 9 (Data Privacy Officer) of this Data Processing Amendment.

11.5. **Termination**. Google will, at least 15 days before appointing any new Third Party Subprocessor, inform Customer of the appointment (including the name and location of such subprocessor and the activities it will perform) either by sending an email to the Notification Email Address or via the Admin Console. If Customer objects to Google's use of any new Third Party Subprocessor, Customer may, as its sole and exclusive remedy, terminate the Google Apps Agreement by giving written notice to Google within 30 days of being informed by Google of the appointment of such subprocessor.

12. **Liability Cap.**

If Google Inc. and Customer (or an authorized Customer Affiliate) enter into Model Contract Clauses as described above, then, subject to the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability), the total combined liability of Google and its Affiliates, on the one hand, and Customer and its Affiliates, on the other hand, under or in connection with the Agreement and all those MCCs combined will be limited to the maximum monetary or payment-based liability amount set out in the Agreement.

13. **Third Party Beneficiary.**

Notwithstanding anything to the contrary in the Agreement, where Google Inc. is not a party to the Agreement, Google Inc. will be a third party beneficiary of Section 6.5 (Auditing Security Compliance), Section 11.3 (Consent to Subprocessing) and Section 12 (Liability Cap) of this Data Processing Amendment.

14. **Effect of Amendment.**

To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, the Agreement remains in full force and effect.

Appendix 1: Categories of Data and Data Subjects

Categories of Data

Personal data submitted, stored, sent or received by Customer or End Users via the Services may include the following categories of data: user IDs, email, documents, presentations, images, calendar entries, tasks and other electronic data

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As of the Amendment Effective Date, Google will take and implement the Security Measures set out in this Appendix to the Data Processing Amendment. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. **Data Center & Network Security.**

(a) **Data Centers.**

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be 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 critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) **Networks & Transmission.**

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or

removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;

2. Employing intelligent detection controls at data entry points; and

3. Employing technologies that automatically remedy certain dangerous situations.

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

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available.

2. **Access and Site Controls.**

(a) **Site Controls.**

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access 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. The fire doors at the data centers are alarmed. 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. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) **Access Control.**

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (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.

3. **Data.**

(a) **Data Storage, Isolation & Authentication**.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per End User basis at the application layer. Google logically isolates each Customer's data, and logically separates each End User's data from the data of other End Users, and data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

The Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to End

Users for specific purposes. Customer may choose to make use of certain logging capability that Google may make available via the Services, products and APIs. Customer agrees that its use of the APIs is subject to the API Terms of Use. Google agrees that changes to the APIs will not result in the degradation of the overall security of the Services.

(b) **Decommissioned Disks and Disk Erase Policy**.

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk 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

4. **Personnel Security.**

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (eg., certifications). Google's personnel will not process Customer Data without authorization.

5. **Subprocessor Security.**

Prior to onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 11.2 (Subprocessing Restrictions) of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Google Apps Data Processing Amendment, Version 1.5