# Data Processing and Security Terms (Enterprise)

These Data Processing and Security Terms, including their appendices (the "Terms") are incorporated into the agreement under which Qwiklabs has agreed to provide Qwiklabs service cloudskillsboost.google/b2b-terms, to the Customer (the "Agreement").

#### 1. Commencement

These Terms will be effective and replace any previously applicable data processing and security terms from the Terms Effective Date (as defined below).

#### 2. Definitions

2.1 Capitalized terms defined in the Agreement apply to these Terms. In addition, in these Terms:

Adequate Country means: (a) for data processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR; (b) for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or (c) for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPA.

<u>Alternative Transfer Solution</u> means a solution, other than SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law.

<u>Customer Data</u> has the meaning given in the Agreement or, if no such meaning is given, means data provided by or on behalf of Customer or Customer End Users via the Services under the Account.

<u>Customer End Users</u> has the meaning given in the Agreement or, if not such meaning is given, has the meaning given to "End Users" in the Agreement.

<u>Customer Personal Data</u> means the personal data contained within the Customer Data, including any special categories of personal data defined under European Data Protection Law.

<u>Customer SCCs</u> means the SCCs (EU Controller-to-Processor) <u>cloudskillsboost.google/scc-eu</u> and/or the SCCs (UK Controller-to-Processor) <u>cloudskillsboost.google/scc-uk</u>, as applicable.

<u>Data Incident</u> means a breach of Qwiklabs' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Qwiklabs.

EEA means the European Economic Area.

<u>EU GDPR</u> means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

<u>European Data Protection Law</u> means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) ("Swiss FDPA").

<u>European or National Law</u> means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and/or (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).

GDPR means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

Instructions has the meaning given in Section 5.2.1 (Customer's Instructions).

Non-European Data Protection Law means data protection or privacy laws in force outside the EEA, the UK and Switzerland.

<u>Notification Email Address</u> means the email address(es) designated by Customer in the Admin Console or Order Form to receive certain notifications from Qwiklabs. Customer is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.

Security Measures has the meaning given in Section 7.1.1 (Qwiklabs' Security Measures).

<u>Subprocessor</u> means a third party authorized as another processor under these Terms to have logical access to and process Customer Data in order to provide parts of the Services.

<u>Supervisory Authority</u> means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; and/or (b) the "Commissioner" as defined in the UK GDPR and/or the Swiss FDPA.

<u>Term</u> means the period from the Terms Effective Date until the earlier of the termination of the Agreement or one year after the expiration of all applicable License Periods for Services under the Agreement including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Qwiklabs may continue providing the Services for transitional purposes.

<u>Terms Effective Date</u> means the date on which Customer accepted, or the parties otherwise agreed to, these Terms.

<u>UK GDPR</u> means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

2.2 The terms "personal data", "data subject", "processing", "controller" and "processor" as used in these Terms have the meanings given in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

#### 3. Duration

Regardless of whether the Agreement has terminated or expired, these Terms will remain in effect until, and automatically expire when, Qwiklabs deletes all Customer Data as described in these Terms.

- 4. Scope of Data Protection Law
- 4.1 <u>Application of European Law</u>. The parties acknowledge that European Data Protection Law will apply to the processing of Customer Personal Data if, for example:
  - the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA or the UK; and/or
  - the Customer Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services in the EEA or the UK, or the monitoring of their behavior in the EEA or the UK.
- 4.2 <u>Application of Non-European Law.</u> The parties acknowledge that Non-European Data Protection Law may also apply to the processing of Customer Personal Data.
- 4.3 <u>Application of Terms</u>. Except to the extent these Terms state otherwise, these Terms will apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

- 5. Processing of Data
- 5.1 Roles and Regulatory Compliance; Authorization.
- 5.1.1 <u>Processor and Controller Responsibilities</u>. If European Data Protection Law applies to the processing of Customer Personal Data:
  - the subject matter and details of the processing are described in Appendix 1;
  - Qwiklabs is a processor of that Customer Personal Data under European Data Protection Law:
  - Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Law; and
  - each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of that Customer Personal Data.
- 5.1.2 <u>Processor Customers</u>. If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants that its instructions and actions with respect to that Customer Personal Data, including its appointment of Qwiklabs as another processor, and Qwiklabs engagement of Subprocessors as described in Section 11, have been authorized by the relevant controller.
- 5.1.3 <u>Responsibilities under Non-European Law</u>. If Non-European Data Protection Law applies to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.
- 5.2 Scope of Processing.
- 5.2.1 <u>Customer's Instructions</u>. Customer instructs Qwiklabs to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services); (c) as documented in the form of the Agreement (including these Terms); and (d) as further documented in any other written instructions given by Customer and acknowledged by Qwiklabs as constituting instructions for purposes of these Terms (collectively, the "Instructions")
- 5.2.2 <u>Qwiklabs's Compliance with Instructions</u>. Qwiklabs will comply with the Instructions described in Section 5.2.1 ("Customer's Instructions") (including with regard to data transfers) unless European or National Law to which Qwiklabs is subject requires other processing of Customer Personal Data by Qwiklabs in which case Qwiklabs will notify Customer (unless that

law prohibits Qwiklabs from doing so on important grounds of public interest) before such other processing.

#### 6. Data Deletion

- 6.1 <u>Deletion by Customer</u>. Qwiklabs will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Qwiklabs to delete the relevant Customer Data from Qwiklabs's systems in accordance with applicable law. Qwiklabs will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European or National Law requires storage.
- Return or Deletion at the end of the Term. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer is responsible for exporting, before the Term expires, any Customer Data it wishes to retain. If Customer does not instruct Qwiklabs to delete or return Customer Data, Qwiklabs will retain the Customer Data for a twelve month period after expiration of all applicable License Periods, as defined in the Agreement, subject to these Terms. If Customer instructs Qwiklabs to delete all remaining Customer Data (including existing copies) from Qwiklabs' systems at the end of the Term in accordance with applicable law, then after a recovery period of up to 30 days from that date, Qwiklabs will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European or National Law requires storage.

# 7. Data Security

- 7.1 <u>Qwiklabs's Security Measures, Controls and Assistance.</u>
- 7.1.1 Qwiklabs's Security Measures. Qwiklabs will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). The Security Measures include measures to encrypt personal data at rest; to help ensure ongoing confidentiality, integrity, availability and resilience of Qwiklabs' systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Qwiklabs may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.
- 7.1.2 <u>Security and Compliance by Qwiklabs Staff</u>. Qwiklabs will: (a) 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; and (b) ensure that all

persons authorized to process Customer Personal Data are under an obligation of confidentiality.

- 7.1.3 <u>Additional Security Controls</u>. Qwiklabs will make Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.
- 7.1.4. <u>Qwiklabs's Security Assistance</u>. Qwiklabs will (taking into account the nature of the processing of Customer Personal Data and the information available to Qwiklabs) assist Customer in ensuring compliance with its obligations under Articles 32 to 34 of the GDPR, by:
  - a) implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Qwiklabs' Security Measures);
  - b) making Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);
  - c) complying with the terms of Section 7.2 (Data Incidents);
  - d) providing Customer with the information contained in the Agreement (including these Terms); and
  - e) if subsections (a)-(d) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

### 7.2 <u>Data Incidents</u>

- 7.2.1 <u>Incident Notification</u>. Qwiklabs will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.
- 7.2.2 <u>Details of Data Incident</u>. Qwiklabs's notification of a Data Incident will describe, to the extent possible, the nature of the Data Incident, the measures taken to mitigate the potential risk and the measures, if any, Qwiklabs recommends that Customer take to address the Data Incident.
- 7.2.3 <u>Delivery of Notification</u>. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address, or at Qwiklabs' discretion, by direct communication (for example, by phone call or an in-person meeting).
- 7.2.4 <u>No Assessment of Customer Data by Qwiklabs</u>. Qwiklabs has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

- 7.2.5 <u>No Acknowledgement of Fault by Qwiklabs</u>. Qwiklabs' notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Qwiklabs of any fault or liability with respect to the Data Incident.
- 7.3 <u>Customer's Security Responsibilities and Assessment.</u>
- 7.3.1 <u>Customer's Security Responsibilities</u>. Without prejudice to Qwiklabs' obligations under Sections 7.1 (Qwiklabs' Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Qwiklabs' or Qwiklabs' Subprocessors' systems, including:
  - using the Services and Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;
  - securing the account authentication credentials, systems and devices Customer uses to access the Services; and
  - retaining or otherwise maintaining appropriate backups of Customer Data as appropriate.
- 7.3.2 <u>Customer's Security Assessment</u>. Customer agrees, based on its current and intended use of the Services, that the Services, Security Measures, Additional Security Controls and Qwiklabs' commitments under this Section 7 (Data Security): (a) meet Customer's needs, including with respect to any security obligations of Customer under European Data Protection Law and/or Non-European Data Protection Law, as applicable, and (b) provide a level of security appropriate to the risk to Customer Data.
- 7.4 Reserved.
- 7.5 Reviews and Audits of Compliance.
- 7.5.1 Reserved.
- 7.5.2 <u>Customer's Audit Rights</u>. If European Data Protection Law applies to the processing of Customer Personal Data, Qwiklabs will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Qwiklabs' compliance with its obligations under these Terms in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). During an audit, Qwiklabs will contribute to the audit as described in this Section 7.5 (Reviews and Audits of Compliance).
- 7.5.3 Additional Business Terms for Reviews and Audits.

- a) Customer must send any requests for audits under Section 7.5.3 or 7.5.2 to Qwiklabs' Data Protection Team as described in Section 12 (Assistance; Processing Records).
- b) Following receipt by Qwiklabs of a request under Section 7.5.3(a), Qwiklabs and Customer will discuss and agree in advance on the reasonable start date, scope and duration of any security and confidentiality controls applicable to any audit.
- c) Qwiklabs may charge a fee (based on Qwiklabs' reasonable costs) for any audit under Section 7.5.2. Qwiklabs will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.
- d) Qwiklabs may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2 if the auditor is, in Qwiklabs' reasonable opinion, not suitably qualified or independent, a competitor of Qwiklabs, or otherwise manifestly unsuitable. Any such objection by Qwiklabs will require Customer to appoint another auditor or conduct the audit itself.
- 7.5.4 <u>No Modification of SCCs</u>. Nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Qwiklabs under any Standard Contract Clauses entered into as described in Section 10 (Transfers of Data).

# 8. Impact Assessments and Consultations

Qwiklabs will (taking into account the nature of the processing and the information available to Qwiklabs) assist Customer in ensuring compliance with its obligations under Articles 35 and 36 of the GDPR, by:

- a) providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);
- b) providing the information contained in the Agreement (including these Terms); and
- c) if subsections (a) and (b) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.
- 9. Access etc.; Data Subject Rights; Data Export
- 9.1 <u>Access: Rectification: Restricted Processing: Portability</u>. During the Term, Qwiklabs will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Qwiklabs as described in Section 6.1 (Deletion by Customer), and to export

Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by applicable European Data Protection Law.

### 9.2 <u>Data Subject Requests</u>.

- 9.2.1 <u>Responsibility for Requests</u>. During the Term, if Qwiklabs receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Qwiklabs will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.
- 9.2.2 <u>Qwiklabs's Data Subject Request Assistance</u>. Qwiklabs will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:
  - a) providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);
  - b) complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and
  - c) if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

### 10. <u>Data Transfers</u>

- 10.1 <u>Data Storage and Processing Facilities</u>. Qwiklabs may store and process Customer Data anywhere Qwiklabs or its Subprocessors maintain facilities, subject to Qwiklabs' obligations under Section 10.3 (Restricted Transfers) below with respect to the Standard Contract Clauses or Alternative Transfer Solution.
- 10.2 <u>Permitted Transfers</u>. The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country ("Permitted Transfers").
- 10.3 <u>Restricted Transfers</u>. If the processing of Customer Personal Data involves any transfers that are not Permitted Transfers, and European Data Protection Law applies to those transfers, then:

- (a) if Qwiklabs announces its adoption of an Alternative Transfer Solution for any Restricted Transfers, then Qwiklabs will ensure that they are made in accordance with that Alternative Transfer Solution; and/or
- (b) if Qwiklabs has not adopted an Alternative Transfer Solution for any Restricted Transfers, then:
- A. the SCCs (EU Controller-to-Processor) will apply with respect to Restricted Transfers between Customer and Google that are subject to the EU GDPR and/or the Swiss FDPA; and
- B. the SCCs (UK Controller-to-Processor) will apply with respect to Restricted Transfers between Customer and Google that are subject to the UK GDPR.
- 10.4 <u>Termination</u>. If Customer concludes, based on its current or intended use of the Services, that the Alternative Transfer Solution and/or SCCs, as applicable, do not provide appropriate safeguards for Customer Personal Data, then Customer may immediately terminate the Agreement for convenience in accordance with the Agreement by notifying Qwiklabs.

## 11. <u>Subprocessors</u>

- 11.1 <u>Consent to Subprocessor Engagement</u>. Customer specifically authorizes the engagement as Subprocessors of all Qwiklabs affiliates from time to time, including Google LLC, Google Cloud EMEA, Google Asia Pacific Pte. Ltd., or any other entity that directly or indirectly controls, is controlled by, or is under common control with Google LLC. In addition, Customer generally authorizes the engagement as Subprocessors of those entities listed as of the Terms Effective Date specified in Section 11.2 (Information about Subprocessors). In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement as Subprocessors of any other third parties ("New Subprocessors").
- 11.2 <u>Information about Subprocessors</u>. Information about Subprocessors, including their functions and locations, is available at <u>cloudskillsboost.google/subprocessors</u> (as such URL may be updated by Qwiklabs from time to time in accordance with these Terms (the "Subprocessor URL").
- 11.3 <u>Requirements for Subprocessor Engagement</u>. When engaging any Subprocessor, Qwiklabs will:
  - ensure via a written contract that:
    - the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Terms); and

- if the processing of Customer Personal Data is subject to European Data Protection Law, the data protection obligations described in these Terms (as referred to in Article 28(3) of the GDPR, if applicable), are imposed on the Subprocessor; and
- remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

### 11.4 Opportunity to Object to Subprocessor Changes.

- When any New Subprocessor is engaged during the Term, Qwiklabs will, at least 60 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform).
- Customer may, within 90 days after being notified of the engagement of a New Subprocessor, object by immediately terminating the Agreement for convenience by notifying Qwiklabs. This termination right is Customer's sole and exclusive remedy if Customer objects to any New Third Party Subprocessor.

# 12. <u>Assistance: Processing Records</u>

- 12.1 <u>Qwiklabs' Assistance</u>. Qwiklabs will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Personal Data under the Agreement and can be contacted at <a href="https://support.google.com/qwiklabs/contact/contact\_us">https://support.google.com/qwiklabs/contact/contact\_us</a> (and/or via such other means as Google may provide from time to time).
- 12.2 <u>Qwiklabs' Processing Records</u>. Qwiklabs will keep appropriate documentation of its processing activities as required by the GDPR. To the extent the GDPR requires Qwiklabs to collect and maintain records of certain information relating to Customer, Customer will use the Admin Console to supply such information and keep it accurate and up-to-date. Qwiklabs may make any such information available to the Supervisory Authorities if required by the GDPR.

### 13. <u>Liability</u>

13.1 <u>Liability Cap</u>. Subject to Section 13.2 (Liability Cap Exclusions), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the Agreement will be limited to the agreed Limitation of Liability under the Agreement for the relevant party.

13.2 <u>Liability Cap Exclusions</u>. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

# 14. <u>Third Party Beneficiary</u>

Notwithstanding anything to the contrary in the Agreement, where Google LLC is not a party to the Agreement, Google LLC will be a third party beneficiary of Sections 7.5 (Reviews and Audits of Compliance), 11.1 (Consent to Subprocessor Engagement) and 13 (Liability).

### 15. <u>Interpretation</u>

- 15.1 Precedence. To the extent of any conflict or inconsistency between:
  - these Terms and the remainder of the Agreement, these Terms will prevail; and
  - any Customer SCCs (which are incorporated by reference into these Terms) and the remainder of the Agreement (including these Terms), the Customer SCCs will prevail.
- 15.2 <u>No Modification of SCCs</u>. Nothing in the Agreement (including these Terms) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

#### Appendix 1: Subject Matter and Details of the Data Processing

### Subject Matter

Qwiklabs provision of the Services to Customer.

#### **Duration of the Processing**

The Term plus the period from the end of the Term until deletion of all Customer Data by Qwiklabs in accordance with the Terms.

#### Nature and Purpose of the Processing

Qwiklabs will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Terms.

#### Categories of Data

Data relating to individuals provided to Qwiklabs via the Services, by (or at the direction of) Customer or by Customer End Users.

The personal data transferred may include the following categories of data:

Contact information: first name, last name, company name, email address; Geo-location information: preferred location, I18n preference, IP address; Information generated by the User through use of the service including Qwiklabs labs progress, classrooms and learning quests, badges, lab completion times, and comments and ratings on labs.

When End Users interact with the Qwiklabs service, the following information is collected from the User's devices:

Standard information sent to web host by browser software (if using a web browser):

IP address:

URL, including referral terms;

Timestamp;

Browser attributes, including browser and OS version inferred from User agent; Information about the content served to a User (advertisement, pages visited, etc.);

Interaction data, like clicks and mouse hovers:

User's preferences and other settings;

Cookie data:

### **Data Subjects**

Data subjects include the individuals about whom data is provided to Qwiklabs via the Services by (or at the direction of) Customer or by Customer End Users.

# Appendix 2: Security Measures

Qwiklabs stores all Customer Data in Google Cloud Storage. As from the Terms Effective Date, Qwiklabs will cause Google to implement and maintain the Security Measures described in this Appendix 2.

1. Data Center and Network Security

#### a) Data Centers.

<u>Infrastructure</u>. Google maintains geographically distributed data centers. Qwiklabs utilizes Google's geographically distributed data centers and 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 Qwiklabs 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, 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 backup generator systems take over. The backup 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.

<u>Server Operating Systems</u>. Qwiklabs servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Qwiklabs 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.

<u>Business Continuity</u>. Qwiklabs relies on Google GCP which has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

b) Networks and Transmission.

<u>Data Transmission</u>. 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. Qwiklabs transfers data via Internet standard protocols.

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

<u>Intrusion Detection</u>. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Qwiklabs' intrusion detection involves:

- tightly controlling the size and make-up of Qwiklabs' attack surface through preventative measures
- employing intelligent detection controls at data entry points; and
- employing technologies that automatically remedy certain dangerous situations.

<u>Incident Response</u>. Qwiklabs monitors a variety of communication channels for security incidents, and Qwiklabs' security personnel will react promptly to known incidents.

<u>Encryption Technologies</u>. Qwiklabs makes HTTPS encryption (also referred to as SSL or TLS connection) available. Qwiklabs servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

#### Access and Site Controls

#### a) Site Controls.

On-site Data Center Security Operation. Google's data centers used by Qwiklabs 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.

<u>Data Center Access Procedures</u>. At the data centers used by Qwiklabs, 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. At the data centers used by Qwiklabs, Google employs 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.

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

<u>Access Control and Privilege Management</u>. Customer's administrators and Customer End Users must create an account and authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.

<u>Internal Data Access Processes and Policies – Access Policy</u>. Qwiklabs' 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. Qwiklabs designs 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. Qwiklabs employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Qwiklabs' authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Qwiklabs with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Qwiklabs 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 Qwiklabs' 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 restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Qwiklabs uses hardware tokens.

### 3. Data

- a) <u>Data Storage. Isolation and Logging</u>. Qwiklabs stores data in a multi-tenant environment on Google-owned servers. Subject to any Instructions to the contrary, Qwiklabs causes Google to replicate Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data. 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 Customer End Users for specific purposes.
- b) <u>Decommissioned Disks and Disk Erase Policy</u>. 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 Qwiklabs' 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

Qwiklabs personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Qwiklabs 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, Qwiklabs' confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., certifications). Qwiklabs' personnel will not process Customer Data without authorization.

# 5. Subprocessor Security

Before onboarding Subprocessors, Qwiklabs 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 Qwiklabs has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement) of these Terms, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.