NON-DISCLOSURE AGREEMENT
REGARDING HIGHLY CONFIDENTIAL INFORMATION AND IMAGES FOR GOOGLE PRODUCTS AND SERVICES

In connection with an engagement between Google LLC ("**Google**") and the party identified below ("**Recipient**") related to the marketing and sale of one or more Google products and services (the "**Purpose**"), Google and Recipient hereby agree:

1. This agreement is effective as of June 2022, or if left blank, the earlier of the two signature dates below.

2. Google (or its affiliates) may disclose to Recipient information related to the Purpose, including images depicting or relating to unreleased Google products, specifications, logos, or other graphics ("**Confidential Information**"). The words "**include**" and "**including**" in this agreement means "including but not limited to." Confidential Information may be disclosed in a variety of forms, including oral presentations, emails, .pdfs, other types of computer files, and as images embedded in presentations. Unless Google specifies otherwise in writing, all information provided to Recipient in connection with the Purpose and anything created by Recipient based on instructions provided by Google will be considered Google's Confidential Information.

3. Recipient will: a) use Confidential Information only for the Purpose and only as it relates to a specific Project (as defined below), b) protect the Confidential Information, c) restrict access to Confidential Information to only Authorized Personnel (as defined below) working on the applicable Project and d) prevent any unauthorized use or disclosure of the Confidential Information. "**Authorized Personnel**" means (i) those employees of Recipient that have signed the Confidentiality Acknowledgement Letter, attached hereto as **Schedule A** (the "**Confidentiality Acknowledgement Letter**") or (ii) those subcontractors that have been pre-approved by Google in writing (email is sufficient) and who (x) have signed a non-disclosure agreement with Google and (y) have had such subcontractor's employees sign the Confidentiality Acknowledgement Letter. "**Project**" means a specific project related to a Google product or service as identified by Google (or its affiliates) (email is sufficient).

4. Recipient may disclose Confidential Information when compelled to do so by law if it provides reasonable prior notice to Google, unless a court orders that Google not be given notice.

5. Confidential Information is highly confidential and must be treated with extreme care to ensure that it is not exposed to third parties or non-Authorized Personnel. Unless otherwise agreed in writing by Google, Recipient and its Authorized Personnel will comply with additional confidentiality terms and the obligations in the attached **Schedule B**.

6. Recipient agrees that Confidential Information will only be shared with or viewed by Authorized Personnel who have a strict need to know in connection with an applicable Project, and only as strictly necessary for the Purpose. Recipient agrees that only such Authorized Personnel will have access to the Confidential Information, and that prior to such access, Recipient will ensure each Authorized Personnel (a) signs an non-disclosure agreement or the Confidentiality Acknowledgement Letter, and (b) is made aware of the contents of this agreement and the sensitivity of the Confidential Information. At all times, Recipient will maintain an up-to-date list of Authorized Personnel for each Project and will collect the signed non-disclosure agreements or Confidentiality Acknowledgement Letters from each Authorized Personnel. Recipient will be responsible with respect to compliance with the terms of this agreement by all Authorized Personnel. Upon Google's request, Recipient will provide an up-to-date list of Authorized Personnel and copies of the signed non-disclosure agreements or Confidentiality Acknowledgement Letter for each Authorized Personnel for each Project. For clarity, Google Confidential Information may only be shared with Authorized Personnel listed for each Project and Google Confidential Information may not be shared with any other personnel not listed by Recipient for that Project.

7. Google (or its affiliates) may reasonably audit Recipient's processes, the list of Authorized Personnel, and workspaces as needed to confirm Recipient's adherence to the requirements in this agreement.

8. Unless otherwise agreed by Google (or its affiliates), Confidential Information may not be printed except as absolutely necessary. If Confidential Information is printed, and keeping in mind that only Authorized Personnel for the applicable Project may see such images, the paper on which the Confidential Information

carlota vilamala

is printed must be either kept in a controlled area so as not to be seen by others or, if it is to be discarded, shredded or otherwise disposed of securely as soon as practicable.

9. Either party may terminate this agreement with thirty days prior written notice to the other party, but this agreement's provisions will survive as to Confidential Information that is disclosed before termination. At any time, Google (or its affiliates) may revoke access to Confidential Information without cause.

10. Unless the parties otherwise agree in writing, Recipient's duty to protect Confidential Information expires the earlier of five years from disclosure or the public launch of the applicable Google product or service depicted in the Confidential Information or identified as part of the Project.

11. This agreement imposes no obligation to proceed with any business transaction.

12. No party acquires any intellectual property rights under this agreement except the limited rights necessary to use the Confidential Information for the Purpose.

13. This agreement does not create any agency or partnership relationship. This agreement is not assignable or transferable by either party without the prior written consent of the other party.

14. Any prior or contemporaneous agreements should be read in concert with this agreement. In the event of a conflict, this agreement will prevail. Any amendments must be in writing. The parties may execute this agreement in counterparts, which taken together will constitute one instrument. Failure to enforce any of the provisions of this agreement will not constitute a waiver.

15. Without prejudice to any other rights or remedies that each party may have, Recipient acknowledges that any breach or threatened breach of this agreement may cause serious loss or damage to Google and/or its affiliates and that monetary damages may not be an adequate remedy for any such breach or threatened breach of the provisions of this agreement. Accordingly, Google will be entitled to apply for specific performance, injunctive relief and any other form of equitable relief or any combination of these remedies to enforce this agreement, in addition to any other available remedies.

16. If any term (or part of a term) of this agreement is invalid, illegal or unenforceable, the rest of the agreement will remain in effect.

17. All notices of termination or breach must be in English, in writing and addressed to the other party's legal department. The address for notices to Google's legal department is legal-notices@google.com. Notice will be treated as given on receipt, as verified by written or automated receipt or by electronic log (as applicable).

18. Recipient acknowledges that the United States securities laws and other laws prohibit any person or entity who has material, non-public information concerning Alphabet Inc. (or its group companies, including Google) from purchasing or selling any of its securities, and from communicating such information to any person or entity under circumstances in which it is reasonably foreseeable that such person is likely to purchase or sell such securities. Recipient will make all persons who receive Confidential information from Recipient under the terms of this agreement aware of this restriction.

19. ALL CLAIMS ARISING OUT OF OR RELATING TO THESE TERMS IN THIS AGREEMENT WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING CALIFORNIA'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA; THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

[Signature page to follow]

carlota vilamala

Google LLC

Signature:_____

Print Name:_____

Title: _____

Address: 1600 Amphitheatre Parkway

Mountain View, California 94043

Date: _____

Recipient: _____
(full company or individual name)

Signature_____

Print Name:_____

Title:_____

Address:_____

_____

Date:_____

carlota vilamala

Schedule A

Confidentiality Acknowledgement Letter

Re: Protection of Google Confidential Information

To the Undersigned ("**you**"):

Google LLC ("**Google**") and your employer identified below ("**Contractor**") have signed a Non-Disclosure Agreement in connection with the marketing and sale of one or more Google products and services (the "**Purpose**") As part of your work on an applicable Project, you may have access to highly confidential information of Google (or its affiliates), including information about Google's products, prototypes, specifications, and business plans, and Google's relationship with Contractor and other companies (collectively, "**Google Confidential Information**"). "**Project**" means a specific project related to a Google product or service as identified by Google (or its affiliates) (email is sufficient) to Contractor. The words "**include**" and "**including**" in this Acknowledgement (as defined below) means "including but not limited to."

To be eligible to work on a Project and in connection with the delivery of any work product (including third party materials) by you or Contractor related to such Project (the "**Deliverable(s)**"), you agree to handle Google Confidential Information 1) in accordance with the terms and obligations in this Confidentiality Acknowledgement Letter (the "**Acknowledgement**"), 2) with the highest level of security, and 3) in connection with the Purpose with only other Authorized Personnel on the same Project in accordance with the Acknowledgement strictly on a **need-to-know** basis. "**Authorized Personnel**" means a list of other authorized personnel maintained by Contractor that have authority to receive Google Confidential Information for a specific Project. **(Initial here_____)**

Requirements for Projects:

1. **Authorized Personnel. (Initial here_____)**
    a. Lead Employees. Contractor departments (e.g. art, engineering, production etc.) will have lead employees who are responsible for specific Project workflows.
    b. Individual Confidentiality Acknowledgement Letter. Each Authorized Personnel that requires access to Google Confidential Information for Projects must sign individual Acknowledgement. You may only share Google Confidential Information with other Authorized Personnel on the same Project, and you will not share or otherwise disclose any Google Confidential Information to any individual that is not an Authorized Personnel for that Project.
    c. Mobile Devices. All Authorized Personnel working on the specific Projects must leave cell phones and any other recording devices outside of Secure Work Areas (as defined below).
    d. Key Card Access. Key card access may be only provided to lead employees and other Authorized Personnel approved in advance by the Google retail team**.**
2. **Facilities. (Initial here_____)**
    a. Secure Work Areas. All work areas involving Projects (e.g., projects with unreleased Google hardware inventory) must have key access entry into secure rooms with limited access to only designated lead employees ("**Secure Work Areas**").

carlota vilamala

b. No Key Access/Restricted Work Areas. If key access is, as required above, not available (e.g., when printing/kitting/assembling), then physical barriers (preferably permanent) to prevent physical and visual working area access (e.g,. tall movable dividing walls or curtains) must be provided with a lead employee checking Authorized Personnel access ("**Restricted Work Areas**").

c. Assembly Areas. Assembly of finished Deliverables must be done, at a minimum, in Restricted Work Areas**.**

d. Storage. Deliverables and any related confidential components (e.g., pre-release marketing assets) must be stored in a secured locations only accessible by Authorized Personnel**.**

e. Transportation. Contractor must establish and document a secure process and chain of custody for transporting any Google asset or other materials used in the creation of Deliverables.

f. Inventory. Contractor will keep a documented inventory of i) Google assets or other materials used in the creation of Deliverables and ii) Deliverables from conception through completion, with written status reports provided to Google upon request**.**

g. Disposal and Recycling. Contractor will recycle or dispose of all Project waste, including packaging and unused parts, in a secure manner, and will retain documentation evidencing such disposal**.**

h. File Transfers. All files must be transferred, whether being transferred to or from Google, via Google Drive. Utilization of third-party services (e.g., Dropbox, Wetransfer) is prohibited**.**

3. **Miscellaneous**. **(Initial here_____)**

a. Google Confidential Information. Unless Google specifies otherwise in writing, all information provided to you and Contractor in association with a Project, including the existence of the Acknowledgement and its purpose, will be considered Google Confidential Information. You agree that during and after your employment with Contractor, you will hold the Google Confidential Information in strictest confidence and only use the Google Confidential Information in accordance with the Acknowledgement and Contractor's agreements with Google. You agree that Google Confidential Information is highly confidential and must be treated with extreme care to ensure that it is not exposed to third parties or non-Authorized Personnel. Upon completion of Google work, you will immediately return to Contractor, or upon Google's or Contractor's request, destroy all Google Confidential Information, including all electronic files, code, documentation, notes, plans, drawings, and copies thereof. You acknowledge that unauthorized disclosure or use of Google Confidential Information during or after your employment with Contractor could cause irreparable harm and significant injury to Google. Accordingly, you agree that Google may seek and obtain immediate injunctive relief against you to enforce Contractor's obligations under its agreement with Google and the Acknowledgement in addition to any other rights and remedies Google may have. At any time, Google may revoke your access to Google Confidential Information without cause.

b. Notice. You will promptly notify Google and Contractor upon discovery of any unauthorized use or disclosure of Google Confidential Information and take all reasonable steps to regain possession of such Google Confidential Information and prevent further unauthorized actions or other breach of the Acknowledgement.

c. Requirements Integration. If Contractor has an Inbound Services Agreement in place with Google as of the signature date below, then these terms and obligations are subject to and incorporated into that Inbound Services Agreement.

d. Severability. If any term (or part of a term) of this Acknowledgement is invalid, illegal or unenforceable, the rest of the Acknowledgement will remain in effect.

carlota vilamala

e. Governing Law. ALL CLAIMS ARISING OUT OF OR RELATING TO THESE TERMS IN THIS LETTER AGREEMENT WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING CALIFORNIA'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA; THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

Acknowledged and agreed.

Name of Authorized Personnel: _____
Signature: _____
Date: _____
Email address of Authorized Personnel: _____
Name of Employer: _____

carlota vilamala

Schedule B

Additional confidentiality terms and the obligations

1. **Additional Definitions**. For the purposes of this agreement:
   a. "**Asset(s)**" means Google asset(s), including images, specifications, messaging, and other information that have not yet been released to the public.
   b. "**Communications**" means any form of communication that contains or relates to, Confidential Information.
   c. "**Deliverables**" means any work product (including third party materials) delivered by Recipient related to a Project (as defined below).
   d. "**Electronic Confidential Information**" means Confidential Information in an electronic format.
   e. "**Physical Confidential Information**" means Confidential Information that is in a physical form including, hard copy or printed materials.

2. **Restrictions.**
   a. Notwithstanding the obligations and restrictions which apply to Confidential Information under this agreement, Recipient will also comply with (and ensure that each Authorized Personnel complies with the obligations and restrictions stated in this Schedule).
   b. Recipient will use an equivalent level of care in safeguarding against disclosure of Google Confidential Information as Recipient uses for Recipient's own highly sensitive confidential information.
   c. Recipient will promptly notify Google upon discovery of any unauthorized use or disclosure of Confidential Information and take all reasonable steps to regain possession of such Confidential Information and prevent further unauthorized actions or other breach of this agreement.
   d. Neither Recipient or any Authorized Personnel may reverse engineer, decompile or disassemble any part of, or remove any proprietary marking from Confidential Information.
   e. Recipient departments (e.g. art, engineering, production etc.) will have lead employees who are responsible for specific workflows.
   f. Key card access may be only provided to lead employees and other Authorized Personnel approved in advance by the Google retail team.
   g. All Authorized Personnel working on a Project must leave cell phones and any other recording devices outside of Secure Work Areas (as defined below).

3. **Physical Confidential Information**. Recipient will ensure that Physical Confidential Information:
   a. is stored in a manner which will ensure confidentiality of the information;
   b. is not co-mingled with any other information held by Recipient;
   c. is not copied or reproduced without the express written permission of Google, except for copies or reproductions that are necessary for the Purpose;
   d. is concealed at all times when being moved and that care is taken to prevent viewing by unauthorized persons; and
   e. that is no longer needed (including any copies or reproductions of such Physical Confidential Information) must be either returned to Google or disposed of by shredding.

4. **Electronic Confidential Information**. Recipient will ensure that Electronic Confidential Information:
   a. is stored in a separate password protected electronic folder and is not co-mingled with any other information held by Recipient including Recipient's own group information or any other information relating to Recipient's supplier, subcontractors, vendors or customers;
   b. is only transmitted using sufficient encryption methods to ensure confidentiality, including the utilization of secured/password protected file storage and dissemination only through non-public email networks;
   c. is not transferred to or stored on portable storage devices including memory drives, USB sticks etc.

carlota vilamala

5. **Assets**. Recipient will ensure that Assets are handled in accordance with the following requirements:
   a. when not in use, Assets will be concealed and stored in an area or space that cannot be accessed by anyone other than the Authorized Personnel;
   b. Assets will not be removed from Recipient's premises or the premises at which Recipient operates except when authorized by Google in writing;
   c. no photographs, drawings or videos will be made of any Assets, unless authorized by Google;
   d. Assets will be promptly returned to Google: (a) when requested by Google; or (b) when no longer needed for the Purpose;
   e. care will be taken when moving Assets to prevent viewing by unauthorized persons (e.g., carrying the Assets in a pouch or another manner of concealment); and
   f. Recipient will report any loss or theft of Assets immediately to Google and take all reasonable steps to regain possession of such Confidential Information and prevent further unauthorized actions or other breach of this agreement.

6. **Communications**. Recipient will ensure that all Communications comply with the following:
   a. where applicable, code names will be used at all times in Communications to protect confidentiality;
   b. any discussion of Confidential Information in public areas is prohibited;
   c. Confidential Information must be removed from any meeting rooms (including information on white boards and printed documents) after a meeting;
   d. the inclusion of Confidential Information in Communications must be limited to that which is necessary for the Purpose;
   e. password protection must be used for all computer stored files and folders when Communications are retained in those files and folders;
   f. all Communications and draft Communications that are no longer needed must be disposed or returned to Google; and
   g. unsecured communication methods (i.e., unattended fax machines) are prohibited.

7. **Destruction/Return of Confidential Information**. Recipient will not be obliged to destroy, return or erase copies of Confidential Information to the extent that Recipient is required to keep that Confidential Information by applicable law, rule or regulation of a professional or regulatory body. Except as otherwise stated in this agreement, if requested in writing by Google, Recipient will immediately:
   a. destroy or return all Confidential Information and any copies made; and
   b. destroy or permanently erase all Confidential Information and any copies made from any computer, word processor or other device containing it.

carlota vilamala

8. **Facilities**.

   a. All work areas involving a Projects (e.g., projects with unreleased Google hardware inventory) must have key access entry into secure rooms with limited access to only designated lead employees ("**Secure Work Areas**").
   b. If key access is, as required above, not available (e.g., when printing/kitting/assembling), then physical barriers (preferably permanent) to prevent physical and visual working area access (e.g,. tall movable dividing walls or curtains) must be provided with a lead employee checking Authorized Personnel access ("**Restricted Work Areas**").
   c. Assembly of finished Deliverables must be done, at a minimum, in Restricted Work Areas.
   d. Deliverables and any related confidential components (e.g., pre-release marketing assets) must be stored in a secured locations only accessible by Authorized Personnel.
   e. Recipient must establish and document a secure process and chain of custody for transporting any Google asset or other materials used in the creation of Deliverables.
   f. Recipient will keep a documented inventory of i) Google assets or other materials used in the creation of Deliverables and ii) Deliverables from conception through completion, with written status reports provided to Google upon request.
   g. Recipient will recycle or dispose of all Project waste, including packaging and unused parts, in a secure manner, and will retain documentation evidencing such disposal.
   h. All files must be transferred, whether being transferred to or from Google, via Google Drive. Utilization of third-party services (e.g., Dropbox, Wetransfer) is prohibited.

9. **Conflict**. In the event of any conflict, the terms of this Schedule will supersede any conflicting terms in the remainder of this agreement.

carlota vilamala