Master Cloud Services Agreement

This Master Cloud Services Agreement (the **"MCSA"**) is entered into as of the Effective Date between Databricks, Inc. ("**Databricks**" or "**we**") and **Customer** (as defined below) and governs Customer's use of the Databricks Services, including the right to access and use the Databricks data processing platform services (the "**Platform Services**"), on each cloud service where Databricks directly provides customers with access to such Platform Services. Please see the Cloud Provider Directory for information relating to these available Cloud Service Providers. For the avoidance of doubt, this Agreement does not govern the use of Databricks Powered Services (as defined below), the use of which is governed by a direct contract between the user and the third party offering the Databricks Powered Service. Unless otherwise indicated, capitalized terms have the meaning assigned to them in this MCSA or in an incorporated Schedule.

If you are entering into this MCSA on behalf of a company (such as your employer) or other legal entity, you represent and warrant that You are authorized to bind that entity to this MCSA, in which case "Customer," "you," or "your" will refer to the Ordering Activity, under GSA Multiple Award Schedule Contracts, identified in the Purchase Order or similar documents . If you do not have authority to bind Your entity or do not agree with any provision of this MCSA, you must not accept this MCSA and may not use the Databricks Services.

By accepting this MCSA, either by executing this MCSA, an Order Form, or another agreement that explicitly incorporates this MCSA by reference, Customer, on behalf of itself and any Affiliates, enters into the MCSA and the following Schedules, each of which are attached hereto and incorporated into the MCSA and apply to the provision of the applicable Databricks Services upon your ordering such service:

- Advisory Services
- Training Services
- U.S. Public Sector Services

Your Order Form (whether entered into directly with Databricks or through a reseller purchasing via a marketplace or similar authorized model) may include specific terms governing the Databricks Services you have ordered, which may include one or more of the following: (a) the Platform Services, (b) contractual volume-based commitment arrangements applicable to any Platform Services or Databricks Powered Service indicated in an Order Form ("**Universal Usage Commitment**"), (c) support services ("**Support Services**"), (d) training services (the "**Training Services**"), or (e) advisory

services (the "**Advisory Services**," and together with any other services provided by Databricks, (a), (b), (c), (d) and (e) shall be defined as the "**Databricks Services**").

1. **Definitions.** Certain terms not defined elsewhere in the Agreement are defined below in this Section. Capitalized terms used but not defined in a Schedule or an Order Form will have the meaning assigned to them, if any, within this MCSA.
    1. **"Acceptable Use Policy"** means the acceptable use policy governing the Platform Services, attached hereto and made available at databricks.com/aup (or such other location as Databricks may provide, and as may be updated from time to time on notice (which notice may be provided by email or within the Platform Services)).
    2. **"Affiliate"** of a party means an entity that controls, is controlled by, or is under common control with such party.
    3. **"Agreement"** means this MCSA, the referenced Schedules, and any accompanying or future Order Form you enter into under this MCSA.
    4. **"Authorized User"** means employees or agents of Customer or Affiliates (or other individuals solely to the extent explicitly permitted in an Order Form) selected by Customer to access and use the Platform Services.
    5. **"BAA"** means a business associate agreement as defined by HIPAA, governing the parties' respective obligations with respect to any PHI that may be contained within Customer Content.
    6. **"Beta Service"** means any Databricks Service (or feature of a Databricks Service) that is clearly designated as "beta", "experimental", "preview" or similar, that is provided prior to general commercial release, and that Databricks at its sole discretion offers to Customer, and Customer at its sole discretion elects to use.
    7. **"Cloud Environment"** of a party means the cloud or other compute or storage infrastructure controlled by the party and utilized under the Agreement.
    8. **"Cloud Provider Directory"** means information relating to the Cloud Service Providers on which Databricks makes available the Platform Services, located at databricks.com/cloud-provider-directory .
    9. **"Cloud Service Provider"** means a cloud service provider on whose platform Databricks directly provides the Platform Services. For clarity, the Databricks Powered Services are not directly provided by Databricks and are not considered Platform Services in the Agreement.

10. **"Compute Plane"** means the portion of the applicable Cloud Environment where compute resources of the Platform Services are deployed during use of the Platform Services for the primary processing of Customer Data. In the case of Serverless Compute, the Compute Plane is within the Databricks Cloud Environment (the "**Databricks Compute Plane**"). In all other cases, the Compute Plane is within the Customer Cloud Environment (the "**Customer Compute Plane**"), and in such cases the processing activity results in fees being charged directly to Customer by the Cloud Service Provider. For the avoidance of doubt, none of the terms "Compute Plane", "Customer Compute Plane" or "Databricks Compute Plane" include Customer's cloud storage. In certain Databricks agreements and Documentation, the Compute Plane may be interchangeably referred to as the "Data Plane".
11. **"Customer Content"** means all Customer Data, Customer Instructional Input, and Customer Results.
12. **"Customer Data"** means the data, other than Customer Instructional Input, made available by Customer and its Authorized Users for processing within the Platform Services or Support Services.
13. **"Customer Instructional Input"** means information other than Customer Data that Customer inputs into the Platform Services to direct how the Platform Services process Customer Data, including without limitation the code and any libraries (including third party libraries) Customer utilizes within the Platform Services.
14. **"Customer Results"** means any output Customer or its Authorized Users generate from their use of the Platform Services.
15. **"Databricks Control Plane"** means the elements of the Platform Services residing within the Databricks Cloud Environment, other than the Databricks Compute Plane, including without limitation the user interface of the Platform Services.
16. **"Databricks Global Code of Conduct"** means the Databricks Global Code of Conduct attached hereto and available at databricks.com/global-code-of-conduct.
17. **"Databricks Powered Service"** means any software or service powered by Databricks Runtime that is provided to you under contract between you and a third party, and this Agreement does not amend any term of such contract; the Databricks Powered Services are not considered Databricks Services (and, for the avoidance of doubt, are not considered Platform Services) under the Agreement and Databricks shall have no liability to you relating to your use of the Databricks Powered Services.

18. **"Databricks Runtime"** means Databricks' proprietary data processing engine, as further described at docs.databricks.com/runtime.
19. **"Documentation"** means the documentation related to the Platform Services located at databricks.com/documentation (or such other location as Databricks may provide, and as may be updated from time to time).
20. **"Effective Date"** means the earliest to occur of: the effective date of the initial Order Form that references this MCSA, the date of last signature of the MCSA, or the date you first access or use any Databricks Services.
21. **"Fees"** means all amounts payable for Databricks Services under an applicable Order Form.
22. **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996, as amended and supplemented from time to time.
23. **"IP Claim"** will have the meaning assigned in Section 6.1 (Indemnification by Databricks).
24. **"Intellectual Property Rights"** means all worldwide intellectual property rights available under applicable laws including without limitation rights with respect to patents, copyrights, moral rights, trademarks, trade secrets, know-how, and databases.
25. **"Monthly PAYG Service"** means the Platform Services provided on a month-to-month basis with payment based only on Customer's usage of the Platform Services during the billing month.
26. **"Order Form"** means an order form, online order (including click-thru setup of any Databricks Services) or similar agreement for the provision of Databricks Services, entered into by the parties, incorporated by reference into, and governed by, the Agreement.
27. **"PCI-DSS"** means the Payment Card Industry Data Security Standard.
28. **"PHI"** means health information regulated by HIPAA or by any similar privacy Law governing the use of or access to health information.
29. **"Platform Services DPA"** means the Platform Services Data Processing Addendum attached hereto and located at databricks.com/dpa.
30. **"Security Addendum"** means the Platform Security Addendum attached hereto and located at databricks.com/security-addendum (or such other location as Databricks may provide, and as may be updated from time to time in accordance with the Agreement).

31. **"Schedule"** means any of the schedules referenced herein or otherwise set forth on an Order Form.
32. **"Serverless Compute"** means a Platform Service where the Compute Plane is located in Databricks' Cloud Environment rather than in Customer's Cloud Environment.
33. **"Service Specific Terms"** means the additional terms applicable to specific Platform Services attached hereto and located at databricks.com/service-specific-terms or such other location as Databricks may provide, and as may be updated from time to time in accordance with the Agreement by Databricks notifying an administrator user within the Platform Services or disclosing the existence of new or changed Service Specific Terms in the applicable section of the Databricks Release Notes (located in the Documentation); Databricks will provide a means by which Customer may subscribe to receive updates to the Service Specific Terms. Service Specific Terms for new Platform Services will be presented for click-through acceptance by an administrator Authorized User prior to enablement of the new Platform Service.
34. **"Support Policy"** means the available Support Services plans attached hereto and as described at databricks.com/support.
35. **"System"** means any application, computing or storage device, or network.
36. **"Workspace"** means a Platform Services environment; a Customer may have multiple Workspaces.

2. **Confidentiality.**
    1. **Confidential Information**. **"Confidential Information"** means any business or technical information disclosed by either party to the other that is designated as confidential at the time of disclosure or that, under the circumstances, a person exercising reasonable business judgment would understand to be confidential or proprietary. Without limiting the foregoing, all non-public elements of the Databricks Services are Databricks' Confidential Information, Customer Content is Customer's Confidential Information, and any information that either party conveys to the other party concerning data security measures, incidents, or findings constitute Confidential Information of both parties. Confidential Information will not include information that the receiving party can demonstrate (a) is or becomes publicly known through no fault of the receiving party, (b) is, when it is supplied, already known to whoever it is disclosed to in circumstances in which they are not prevented from disclosing it to others, (c) is independently obtained by whoever it is disclosed to in circumstances in which they are not prevented from disclosing it to

others or (d) was independently developed by the receiving party without use of or reference to the Confidential Information.

2. **Confidentiality.** A receiving party will not use the disclosing party's Confidential Information except as permitted under the Agreement or to enforce its rights under the Agreement and will not disclose such Confidential Information to any third party except to those of its employees and/or subcontractors who have a bona fide need to know such Confidential Information for the performance or enforcement of the Agreement; provided that each such employee and/or subcontractor is bound by a written agreement that contains use and disclosure restrictions consistent with the terms set forth in this Section 2.2. Each receiving party will protect the disclosing party's Confidential Information from unauthorized use and disclosure using efforts equivalent to those that the receiving party ordinarily uses with respect to its own Confidential Information of similar nature and in no event using less than a reasonable standard of care; provided, however, that a party may disclose such Confidential Information as required by applicable laws, subject to the party required to make such disclosure giving reasonable notice to the other party to enable it to contest such order or requirement or limit the scope of such request. The provisions of this Section 2.2 will supersede any non-disclosure agreement by and between the parties and/or their Affiliates (whether entered into before, on or after the Effective Date) that would purport to address the confidentiality and security of Customer Content (including 'customer data' regardless of how defined) and such agreement will have no further force or effect with respect to Customer Content. Databricks recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.
3. **Reserved**.

3. **Intellectual Property.**
    1. **Ownership of the Databricks Services**. Except for the limited licenses expressly set forth in the Agreement, Databricks retains all Intellectual Property Rights and all other proprietary rights related to the Databricks Services. You will not delete or alter the copyright, trademark, or other proprietary rights notices or markings appearing within the Databricks Services as delivered to you. You agree that the Databricks Services are provided on a non-exclusive basis and that no transfer of ownership of Intellectual Property Rights will occur. You further acknowledge and agree that portions of the Databricks Services, including but not limited to the source code and

the specific design and structure of individual modules or programs, constitute or contain trade secrets and other Intellectual Property Rights of Databricks and its licensors.

2. **Ownership of Customer Content**. As between you and Databricks, you retain all ownership or license rights in Customer Content.
3. **Feedback.** You are under no duty to provide any suggestions, enhancement requests, or other feedback regarding the Databricks Services ("**Feedback**"). If you choose to offer Feedback to Databricks, you hereby grant Databricks a perpetual, irrevocable, non-exclusive, worldwide, fully-paid, sub-licensable, assignable license to incorporate into the Databricks Services or otherwise use any Feedback Databricks receives from you solely to improve Databricks products and services, provided that such Feedback is used in a manner that is not attributable to you. You also irrevocably waive in favor of Databricks any moral rights which you may have in such Feedback pursuant to applicable copyright law. Databricks acknowledges that any Feedback is provided on an "as-is" basis with no warranties of any kind.

4. **Use of the Platform Services.**
    1. **Access and Support**.
        1. **Use Authorization**. If your Order Form includes Platform Services or you have created a Platform Services account through online setup, you and your Authorized Users may, subject to the terms of such Order Form and the Agreement, including any applicable Schedule or addendum, access and use the Platform Services on any permitted Cloud Service Provider solely for your internal business purposes; if such rights have not been expressly provided to you, you may not use the Platform Services and this Section 4 (Use of the Platform Services) does not apply.
        2. **Cloud Service Providers**. A list of, and applicable information relating to the use of the Platform Services on, available Cloud Service Providers is set forth in the Cloud Provider Directory which is incorporated into the Agreement by reference. Databricks may add additional Cloud Service Providers at any time. Instructions on how you may use the Platform Services on the new Cloud Service Provider without needing to enter into a new Order Form may, as applicable, be provided on the Cloud Provider Directory or within a given Order Form.
        3. **Modifications; No Material Diminishment**. Databricks reserves the right to improve or otherwise modify the Platform Services and its System architecture or update the Service Specific Terms or Security Addendum at any time subject to

maintaining appropriate industry standards of practice relating to the provision and security of the Platform Services, and provided that any such modification (including any modification to the Service Specific Terms or the Security Addendum) does not materially diminish the core functionality or security of the Platform Services.

4. **Selecting Authorized Users**. You must obtain separate credentials (e.g., user IDs and passwords) via the Platform Services for each Authorized User and may not permit the sharing of Authorized User credentials.
5. **Your Responsibilities Regarding Authorized Users**. You will at all times be responsible for and expressly assume the risks associated with all use of the Platform Services under an Authorized User's account (including for the payment of Fees related to such use), whether such action was taken by an Authorized User or by another party, and whether or not such action was authorized by an Authorized User, provided that such action was not (1) taken by Databricks or by a party acting under the direction of Databricks, or (2) an action by a third party that Databricks should reasonably have prevented. This responsibility includes the security of each Authorized User's credentials, and you will not share (and will instruct each Authorized User not to share) such credentials with any other person or entity, or otherwise permit any other person or entity to access or use the Platform Services, except to the extent permitted in an Order Form.
6. **Support Services**. Databricks will provide you with the level of Support Services specified on an Order Form in accordance with the Support Policy. If Support Services are not specified on an Order Form, your support shall be limited to public Documentation and forums.

2. **Use Limits**. You will not, and will not permit your Authorized Users to:
    1. violate the Acceptable Use Policy or use the Platform Services other than in accordance with the Documentation;
    2. copy, modify, disassemble, decompile, reverse engineer, or attempt to view or discover the source code of the Platform Services, in whole or in part, or permit or authorize a third party to do so, except to the extent such activities are expressly permitted by the Agreement or by law notwithstanding this prohibition;
    3. sell, resell, license, sublicense, distribute, rent, lease, or otherwise provide access to the Platform Services to any third

party except to the extent explicitly authorized in writing by Databricks;

4. use the Platform Services to develop or offer a service made available to any third party that could reasonably be seen to serve as a substitute for such third party's possible purchase of any Databricks product or service;
5. transfer or assign any of your rights hereunder except as permitted under Section 11.4 (Assignment) of the MCSA; or
6. during any free trial period granted by Databricks, including during the use of any Beta Service, use the Databricks Services for any purpose other than to evaluate whether to purchase the Databricks Services.

3. **Customer Content**.
    1. **Limits on What Customer Content May Contain**. You agree that you may not include in Customer Data or Customer Instructional Input, or generate any Customer Results that include:
        1. any data for which you do not have all rights, power and authority necessary for its collection, use and processing as contemplated by the Agreement;
        2. any data that is prohibited by the Acceptable Use Policy;
        3. any PHI unless (1) you are processing the PHI in a PHI Permitted Workspace and configure and operate such Workspace in accordance with the Documentation; and (2) you have entered into (a) an Order Form that explicitly permits you to process PHI within the Platform Services, and then only with respect to the Workspace(s) identified in such Order Form (the "**PHI Permitted Workspaces**"); and (b) if you are a Covered Entity or a Business Associate (each as defined under HIPAA), a BAA with Databricks which, upon mutual execution, will be incorporated by reference into and subject to the Agreement. If you have not entered into a BAA with Databricks or if you provide PHI to Databricks other than through the PHI Permitted Workspaces, Databricks will have no liability under the Agreement relating to PHI, notwithstanding anything in the Agreement or in HIPAA or any similar laws to the contrary;
        4. any cardholder data as defined under PCI-DSS ("**Cardholder Data**") unless (1) you are processing the Cardholder Data in a PCI Permitted Workspace and

configure and operate such Workspace in accordance with the Documentation; and (2) you have entered into an Order Form that (a) specifies Databricks then-current certification status under PCI-DSS; and (b) explicitly permits you to process Cardholder Data within the Platform Services (including specifying the types and quantities of such data) and, and then only with respect to the Workspace(s) identified in such Order Form (the "**PCI Permitted Workspaces**"). If you have not entered into such mutually executed Order Form with Databricks, or if you provide Cardholder Data to Databricks other than through the PCI Permitted Workspaces, Databricks will have no liability under the Agreement relating to Cardholder Data, notwithstanding anything in the Agreement or in PCI-DSS or any similar regulations to the contrary.

2. **Usage Data**. You acknowledge and agree that, notwithstanding anything to the contrary in the Agreement, Databricks may collect usage data and telemetry regarding your Authorized Users' use of the Platform Services and that such usage data may occasionally contain Customer Instructional Input (e.g., it may contain the queries entered by an Authorized User) but will not contain Customer Data or Customer Results ("**Usage Data**"). Databricks will not share (other than with third parties providing services to Databricks who agree in writing to terms at least as restrictive regarding the processing of Usage Data as those set forth in the Agreement) or publicly make available any Usage Data that identifies Customer, or any of its Authorized Users, other data subjects, or customers, nor use any Usage Data in a manner that derives its value from the unique aspects of your Customer Instructional Input.

4. **Security; Data Protection**.
    1. **Shared Responsibility**. Customer acknowledges that the Platform Services are implemented in a manner that divides the Platform Services between the Customer Cloud Environment and the Databricks Cloud Environment, and that accordingly each party must undertake certain technical and organizational measures in order to protect the Platform Services and the Customer Content. Without limiting the foregoing, Customer acknowledges and agrees that (1) in order to utilize the current Platform Services other than Serverless Compute, Customer must have an account with

the applicable Cloud Service Provider; (2) Databricks does not host the Customer Cloud Environment into which certain parts of the Platform Services may be deployed or the Systems in which your Customer Data may be stored (e.g., an AWS S3 bucket); (3) while certain Customer Data may in some cases be present within the Databricks Cloud Environment of the Platform Services (e.g., within the Customer Results), Databricks' current Platform Services are not designed to archive or permanently retain Customer Data (e.g., they are intended to provide an environment to facilitate Customer's processing of Customer Data by permitting Customer to execute Customer Instructional Input and view Customer Results); and (4) Databricks' current Platform Services do not provide backup services to enable recovery of Customer Data. Accordingly, and without limiting the foregoing, Databricks is not responsible for any loss, destruction, alteration, or corruption of Customer Content, except to the extent caused by the gross negligence or willful misconduct of Databricks.

2. **Different Architectures**. Databricks provides the Platform Services according to different architectural models depending on the specific feature being used by Customer, as further described in the Documentation. Accordingly, Customer acknowledges and agrees that different portions of the Platform Services are and may in the future be subject to Service Specific Terms that provide for different rights and responsibilities of the parties.
3. **Databricks Responsibilities**. Databricks acknowledges and agrees that, as between the parties and except to the extent caused by the action or intentional or negligent inaction of you or your Authorized Users, including without limitation any customizations or configurations of the Platform Services by you or anything specified to be your responsibility above, Databricks is primarily responsible for the operation (excluding to the extent such operation is directed by the Customer Instructional Input) of the Databricks Cloud Environment (including the user interface of the Platform Services, the Databricks Compute Plane with respect to Serverless Compute, and the portion of the Platform Services within the Databricks Control Plane in which the Customer Instructional Input and Customer Results are held until deleted by you) and, with respect to Platform Services other than Serverless Compute, the Databricks software that operates the computing resources in the Customer Compute Plane.

Databricks shall implement reasonable administrative, physical, and technical safeguards to protect the security of the Platform Services and the Customer Content as set forth in the Security Addendum ("**Security Measures**"); and shall, without limiting the foregoing, maintain throughout the term of the Agreement certification to ISO/IEC 27001:2013 or equivalent/greater standards. Additionally, while it is your responsibility to back up Customer Instructional Input, Databricks will, at your reasonable request, provide commercially reasonable assistance with recovery efforts where reasonably possible.

4. **Customer Responsibilities**. You acknowledge and agree that you are responsible for:
    1. protecting the security of all your credentials used to access the Platform Services (with Databricks also responsible for taking adequate steps to protect Customer credentials to the extent such credentials are within the control of Databricks);
    2. securing the Customer Cloud Environment, including without limitation the Customer Compute Plane, and any Customer System (with such steps to include without limitation the regular rotation of access keys and other industry standard steps to preclude unauthorized access);
    3. backing up Customer Instructional Input (e.g., via Github or other third party System);
    4. all Customer Instructional Input and any consequences arising from Databricks' execution of such Customer Instructional Input except to the extent caused by Databricks' breach of its Security Measures or gross negligence or willful misconduct;
    5. backing up and securing Customer Data under Customer's control within the Customer Cloud Environment or other Customer controlled System (e.g., by turning on versioning and encryption within AWS S3);
    6. configuring the Platform Services in an appropriate way taking into account the sensitivity of the Customer Content that you choose to process using the Platform Services;
    7. using commercially reasonable efforts to ensure that your Authorized Users review the portions of Documentation relevant to your use of the Platform

Services and any security information published by Databricks and referenced therein that is designed to assist you in securing Customer Content;

8. complying with your security obligations as set forth in the Agreement, including any applicable Schedule or addendum;
9. managing and paying the charges associated with your usage of the Customer Cloud Environment (e.g., compute and storage fees); and
10. ensuring that Databricks at all times has updated and accurate contact information for the appropriate person for Databricks to notify regarding data security issues relating to the Databricks Services, with such contact information to be updated in each Order Form and any subsequent changes to be provided by email to customercontact@databricks.com (with "Contact Detail Change" in the subject) and Customer expressly assumes the risks associated with the responsibilities set forth above in this Section;

5. **Platform Services DPA**. Except with respect to a free trial, the terms of the Platform Services DPA are attached hereto and shall apply to the extent Customer Content includes Personal Data, as defined in the Platform Services DPA.

5. **Suspension and Termination of Platform Services**.
    1. **Suspension**. **Reserved**.
    2. **Termination; Workspace Cancellation**. If the Agreement or any applicable Order Form or Schedule is terminated for any reason or upon your written request, Databricks may cancel your Workspaces. Upon termination of the Agreement for any reason, you will delete all stored elements of the Platform Services from your Systems.
    3. **Deletion of Customer Content upon Workspace Cancellation**. Databricks will delete all Customer Content contained within a Workspace within thirty (30) days following the cancellation of such Workspace.
    4. **Monthly PAYG Services**. Notwithstanding anything in the Agreement to the contrary, Databricks may suspend or terminate any Monthly PAYG Services Workspace, and delete any Customer Content relating to such Workspace that may be stored within the Platform Services or other Databricks' Systems, upon thirty (30) day's prior written notice (email

sufficient) if Databricks reasonably determines the account is inactive as set forth in the Acceptable Use Policy.

5. **Notice**. Notwithstanding Section 11.5 (Notice) of the MCSA, notice under this Section 4.5 (Suspension; Termination) may be provided by email sent to the Ordering Activity's Contracting Officer who signed the applicable Purchase Order.

5. **Warranties; Remedy.**
    1. **Warranties**. Each party warrants that it is validly entering into the Agreement and has the legal authority to do so. In addition to the warranties provided by the parties as set forth in any applicable Schedule, Databricks warrants that, during the term of any Order Form for Platform Services: (a) the Platform Services will function substantially in accordance with the Documentation; and (b) Databricks will employ commercially reasonable efforts in accordance with industry standards to prevent the transmission of malware or malicious code via the Platform Services.
    2. **Disclaimer**. THE WARRANTIES PROVIDED BY DATABRICKS IN SECTION 5.1 (WARRANTIES) ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, REGARDING DATABRICKS AND DATABRICKS' SERVICES PROVIDED HEREUNDER. DATABRICKS AND ITS LICENSORS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES, CONDITIONS AND OTHER TERMS, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE. NOTWITHSTANDING ANYTHING TO THE CONTRARY HEREIN: (a) ANY SERVICES PROVIDED UNDER ANY FREE TRIAL PERIOD ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND; (b) WITHOUT LIMITATION, DATABRICKS DOES NOT MAKE ANY WARRANTY OF ACCURACY, COMPLETENESS, TIMELINESS, OR UNINTERRUPTABILITY, OF THE PLATFORM SERVICES; (c), DATABRICKS IS NOT RESPONSIBLE FOR RESULTS OBTAINED FROM THE USE OF THE DATABRICKS SERVICES OR FOR CONCLUSIONS DRAWN FROM SUCH USE; AND (d) EXCEPT AS OTHERWISE STATED IN SECTION 4 (USE OF THE PLATFORM SERVICES), DATABRICKS' REASONABLE EFFORTS TO RESTORE LOST OR CORRUPTED CUSTOMER INSTRUCTIONAL INPUT DESCRIBED THEREIN SHALL BE DATABRICKS' SOLE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF ANY LOSS OR CORRUPTION OF CUSTOMER

CONTENT IN CONNECTION WITH THE DATABRICKS SERVICES.

3. **Platform Services Warranty Remedy**. FOR ANY BREACH OF THE WARRANTIES RELATED TO THE PLATFORM SERVICES PROVIDED BY DATABRICKS IN SECTION 5.1 (WARRANTIES), YOUR EXCLUSIVE REMEDY AND DATABRICKS' ENTIRE LIABILITY WILL BE THE MATERIAL CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR, IF WE CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER, DATABRICKS WILL END THE DEFICIENT SERVICES AND REFUND TO YOU THE PORTION OF ANY PREPAID FEES PAID BY YOU TO DATABRICKS APPLICABLE TO THE PERIOD FOLLOWING THE EFFECTIVE DATE OF TERMINATION.

6. **Indemnification.**
    1. **Indemnification by Databricks**. Subject to Section 6.5 (Conditions of Indemnification), Databricks may participate in the defense of the Customer against any claim, demand, suit or proceeding made or brought against Customer by a third party (a "**Claim Against Customer**") alleging that the Databricks Services as provided to Customer by Databricks or Customer's use of the Databricks Services in accordance with the Documentation and the Agreement infringes or misappropriates such party's Intellectual Property Rights (an "**IP Claim**"), and will indemnify Customer from and against any damages, attorney fees and costs finally awarded against Customer as a result of, or for amounts paid by Customer under a settlement approved by Databricks in writing of, a Claim Against Customer. Notwithstanding the foregoing, Databricks will have no liability for any infringement or misappropriation claim of any kind if such claim arises from: (a) the public open source version of Apache Spark (located at github.com/apache/spark), if the claim of infringement or misappropriation does not allege with specificity that the infringement or misappropriation arises from the Platform Services (as opposed to Apache Spark itself); (b) the combination, operation or use of the Databricks Services with equipment, devices, software or data (including without limitation your Confidential Information) not supplied by Databricks, if a claim would not have occurred but for such combination, operation or use; or (c) your or an Authorized User's use of the Databricks Services other than in accordance with the Documentation and the Agreement.
    2. **Other Remedies**. If Databricks receives information about an infringement or misappropriation claim related to a Databricks Service or otherwise becomes aware of a claim that the provision of

any of the Databricks Services is unlawful in a particular territory, then Databricks may at its sole option and expense: (a) replace or modify the applicable Databricks Services to make them non-infringing and of substantially equivalent functionality; (b) procure for you the right to continue using the Databricks Services under the terms of the Agreement; or (c) if Databricks is unable to accomplish either (a) or (b) despite using its reasonable efforts, terminate your rights and Databricks' obligations under the Agreement with respect to such Databricks Services and refund to you any Fees prepaid by you to Databricks for Databricks Services not yet provided.

3. **Indemnification by Customer**. **Reserved**.
4. **Sole Remedy**. SUBJECT TO SECTION 6.5 (CONDITIONS OF INDEMNIFICATION) BELOW, THE FOREGOING SECTIONS 6.1 (INDEMNIFICATION BY DATABRICKS) AND 6.2 (OTHER REMEDIES) STATE THE ENTIRE OBLIGATION OF DATABRICKS AND ITS LICENSORS WITH RESPECT TO ANY ALLEGED OR ACTUAL INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS BY THE DATABRICKS SERVICES.
5. **Conditions of Indemnification**. As a condition to an indemnifying party's (each, an "**Indemnitor**") obligations under this Section 6 (Indemnification), a party seeking indemnification (each, an "**Indemnitee**") will: (a) promptly notify the Indemnitor of the claim for which the Indemnitee is seeking indemnification (but late notice will only relieve Indemnitor of its obligation to indemnify to the extent that it has been prejudiced by the delay); (b) allow the Indemnitor to participate in the defense (including selection of counsel) and settlement of the claim; (c) provide the Indemnitor, at the Indemnitor's expense, with all assistance, information and authority reasonably required for the defense and settlement of the claim; and (d) preserve and will not waive legal, professional or any other privilege attaching to any of the records, documents, or other information in relation to such claim without prior notification of consent by the Indemnitor. The Indemnitor will not settle any claim in a manner that does not fully discharge the claim against an Indemnitee or that imposes any obligation on, or restricts any right of, an Indemnitee without the Indemnitee's prior written consent, which may not be unreasonably withheld or delayed. An Indemnitee has the right to retain counsel, at the Indemnitee's expense, to participate in the defense or settlement of any claim. The Indemnitor will not be liable for any settlement or compromise that an Indemnitee enters into without the Indemnitor's prior written consent.

7. **Limitation of Liability.**
    1. EXCEPT WITH RESPECT TO (I) LIABILITY THAT CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAWS, (II) LIABILITY ARISING OUT OF FRAUD OR FRAUDULENT MISREPRESENTATION, OR (III) CUSTOMER'S INDEMNIFICATION OBLIGATIONS, NEITHER PARTY WILL HAVE ANY LIABILITY FOR: (A) INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL LOSS OR DAMAGES; (B) LOST PROFITS OR REVENUE; (C) LOSS FROM DAMAGE TO BUSINESS OR GOODWILL; (D) LOSS OF DATA; OR (E) LOSS ARISING FROM INACCURATE OR UNEXPECTED RESULTS ARISING FROM THE USE OF THE DATABRICKS SERVICES, REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES ARISING.
    2. SUBJECT TO SECTIONS 7.1, 7.3, 7.4 AND 7.5, EXCEPT WITH RESPECT TO LIABILITY ARISING OUT OF: (I) PERSONAL INJURY OR DEATH CAUSED BY THE NEGLIGENCE OF A PARTY, ITS EMPLOYEES, AFFILIATES, OR AGENTS; (II) DATABRICKS' INDEMNIFICATION OBLIGATIONS FOR AN IP CLAIM; OR (III) CUSTOMER'S INDEMNIFICATION OBLIGATIONS, IN NO EVENT WILL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THE AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES FOR THE DATABRICKS SERVICES GIVING RISE TO THE LIABILITY IN THE TWELVE (12) MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE (THE "**GENERAL CAP**"). THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, BUT WILL NOT LIMIT CUSTOMER'S AND ITS AFFILIATES' PAYMENT OBLIGATIONS UNDER SECTION 9 (PAYMENT). THIS AGREEMENT SHALL NOT IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733. FURTHERMORE, THIS CLAUSE SHALL NOT IMPAIR NOR PREJUDICE THE U.S. GOVERNMENT'S RIGHT TO EXPRESS REMEDIES PROVIDED IN THE GSA SCHEDULE CONTRACT (E.G., CLAUSE 552.238-81 – PRICE REDUCTIONS, CLAUSE 52.212-4(H) – PATENT INDEMNIFICATION, AND GSAR 552.215-72 – PRICE

ADJUSTMENT – FAILURE TO PROVIDE ACCURATE INFORMATION).

3. SUBJECT TO SECTIONS 7.1, 7.4 AND 7.5, DATABRICKS' AGGREGATE LIABILITY FOR ANY CLAIMS OR DAMAGES, DIRECT OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH DATABRICKS' BREACH OF ITS CONFIDENTIALITY OBLIGATIONS (SECTION 2.2) OR, WITH RESPECT TO THE PROVISION BY DATABRICKS OF THE PLATFORM SERVICES (IF APPLICABLE), THE DATA PROTECTION AND SECURITY OBLIGATIONS SET FORTH IN SECTION 4.4(c) (DATABRICKS RESPONSIBILITIES) OR THE PLATFORM SERVICES DPA, WHERE SUCH BREACH RESULTS IN UNAUTHORIZED DISCLOSURE OF CUSTOMER CONTENT, EXCEPT TO THE EXTENT SUCH CLAIMS OR DAMAGES ARE CAUSED BY DATABRICKS' GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, SHALL BE LIMITED TO TWO (2) TIMES THE GENERAL CAP ("**DATA PROTECTION CLAIMS CAP**").
4. IN NO EVENT SHALL DATABRICKS BE LIABLE FOR THE SAME EVENT UNDER BOTH THE GENERAL CAP AND THE DATA PROTECTION CLAIMS CAP. SIMILARLY, THOSE CAPS SHALL NOT BE CUMULATIVE; IF THERE ARE ONE OR MORE CLAIMS SUBJECT TO EACH OF THOSE CAPS, THE MAXIMUM TOTAL LIABILITY FOR ALL CLAIMS IN THE AGGREGATE SHALL NOT EXCEED THE DATA PROTECTION CLAIMS CAP.
5. NOTWITHSTANDING ANYTHING CONTAINED ABOVE, ANY LIABILITY RELATING TO BETA SERVICES OR ANY DATABRICKS SERVICES PROVIDED FREE OF CHARGE, INCLUDING ANY DATABRICKS SERVICES PROVIDED DURING A FREE TRIAL PERIOD, WILL BE LIMITED TO FIVE THOUSAND US DOLLARS (USD $5,000).

8. **Term**
    1. **Term of Agreement.** The Agreement will become effective on the Effective Date and will continue in full force and effect until terminated by either party pursuant to this Section 8 (Term). The Agreement may be terminated (i) by either party on thirty (30) days' prior written notice if there are no operative Order Forms outstanding.
    2. **Term of Order Forms.** The Term of an Order Form will be as specified in the Order Form.
    3. **Survival.** All provisions of the Agreement that by their nature should survive termination will so survive.
9. **Payment.** Reserved.

10. **Compliance with Laws.**
    1. **By Databricks Generally**. Databricks will provide the Databricks Services in accordance with its obligations under laws and government regulations applicable to Databricks' provision of the Databricks Services to its customers generally, including, without limitation those related to data protection and data privacy, irrespective of Customer's particular use of the services.
    2. **By Customer Generally**. You represent and warrant to Databricks that your use of Databricks Services will comply with all applicable laws and government regulations, including without limitation those related to data protection and data privacy.
    3. **Export Controls; Trade Sanctions**. The Databricks Services may be subject to export controls and trade sanctions laws of the United States and other jurisdictions. Customer acknowledges and agrees that it will comply with all applicable export controls and trade sanctions laws, regulations and/or any other relevant restrictions in Customer's use of the Databricks Services, including that you will not permit access to or use of any Databricks Services in any country where such access or use is subject to a trade embargo or prohibition, and that you will not use Databricks Services in support of any controlled technology, industry, or goods or services without having a valid governmental license, authority, or permission to engage in such conduct. Each party further represents that it is not named on any governmental or quasi-governmental denied party or debarment list that would restrict access to, or use or delivery of, the Databricks Services, including without limitation lists maintained by the U.S. Department of Commerce, U.S. Department of State, U.S. Department of Treasury, or other agency.
    4. **Business Practices; Code of Conduct**. Databricks maintains a set of business practice principles and policies in the Databricks Global Code of Conduct, which employees are required to follow. Databricks will abide by these principles and policies in the conduct of all business for Customer and expects your use of any Databricks Services to be conducted utilizing principles of business ethics and social responsibility and, with respect to any Platform Services, in accordance with Databricks' Acceptable Use Policy and the applicable Platform Services terms set forth in the Agreement.
11. **General.**
    1. **Governing Law and Venue.** This Agreement is governed by Federal law. In all cases, the application of law will be without regard to, or application of, conflict of law rules or principles, and the United Nations Convention on Contracts for the International Sale of Goods will not apply.

2. **Insurance Coverage.** Databricks will maintain commercially appropriate insurance coverage given the nature of the Databricks Services and Databricks' obligations under the Agreement. Such insurance will be in an industry standard form with licensed insurance carriers with A.M. Best ratings of A-IX or better, and will include commercially appropriate cyber liability insurance coverage. Upon request, Databricks will provide Customer with certificates of insurance evidencing such coverage.

3. **Entire Agreement, Construction, Amendment and Execution.** The Agreement (including any attached Schedule) is the complete and exclusive understanding and agreement between the parties regarding its subject matter. In the event there is a conflict between any provision in a Purchase Order, this MCSA, a Schedule, Addendum, Policy, or other document, the conflict shall be resolved in accordance with General Services Administration Acquisition Regulation 552.212-4(s) Order of Precedence. If any provision of the Agreement is held to be unenforceable or invalid, the other provisions will remain in full force and effect. The headings in the Agreement and the Schedules are solely for convenience and will not be taken into consideration in interpretation of the Agreement. Any translation of the Agreement or an Order Form that is provided as a courtesy shall not be legally binding and the English language version will always prevail. The Agreement may not be modified or amended except by mutual written agreement of the parties. The Agreement may be executed in two or more counterparts, each of which will be deemed an original and all of which, taken together, will constitute one and the same instrument. A party's electronic signature or transmission of any document by electronic means will be deemed to bind such party as if signed and transmitted in physical form.
4. **Assignment. Reserved**.
5. **Notice.** Any required notice under the Agreement will be deemed given when received by letter delivered by nationally recognized overnight delivery service or recorded prepaid mail. Unless notified in writing of a change of address, you will send any required notice to Databricks, Inc., 160 Spear Street, Suite 1300, San Francisco, CA 94105, USA, attention: Legal Department, or to the alternative Databricks Affiliate (if any) identified in an applicable Order Form, and Databricks will send any required notice to you directed to the most recent address you have provided to Databricks for such notice.

6. **Force Majeure.** In accordance with GSAR 552.212-4(f), Neither party will be liable or responsible to the other party nor be deemed to have defaulted under or breached the Agreement for any failure or delay in fulfilling or performing any term of the Agreement (except for any obligations to make payments to the other party), when and to the extent such failure or delay is caused by or results from acts beyond the impacted party's ("**Impacted Party**") reasonable control, including without limitation the following force majeure events ("**Force Majeure Event(s)**"): (a) acts of God, (b) acts of government, including any changes in law or regulations, (c) acts or omissions of third parties, (d) flood, fire, earthquakes, civil unrest, wars, acts of terror, pandemics, or strikes or other actions taken by labor organizations, (e) computer, telecommunications, the Internet, Internet service provider or hosting facility failures or delays involving hardware, software or power systems not within the Impacted Party's possession or reasonable control, (f) network intrusions or denial of service attacks, or (g) any other cause, whether similar or dissimilar to any of the foregoing, that is beyond the Impacted Party's reasonable control.

Approved by GSA 5 April 2023

Databricks Support Tiers

Databricks provides a number of plans that provide you with dedicated support
and timely service for the Databricks platform and Apache Spark.

FEATURE
MULTI-CLOUD SUPPORT Support for Databricks on permitted Cloud Service Providers and Databricks-Powered Services; Complimentary Success Credits available based on commitment size
SINGLE-CLOUD SUPPORT Support for Platform Services on a single-chosen Cloud Service Provider
SUPPORT PORTAL ACCESS Online repository of documentation, guides, best practices, and more.
UPDATES & PATCHES Receive updates, bug fixes, and patches without impact to your business.
SERVICE LEVEL AGREEMENT Receive support responses according to issue severity.
STANDARD SUPPORT SEVERITY 1 Production system is down or severely impacted such that routine operation is impossible
STANDARD SUPPORT SEVERITY 2 Production issue where the system is functioning but in degraded or restricted capacity
STANDARD SUPPORT SEVERITY 3

FEATURE
Issue where minor functionality is impacted or a development issue occurs
STANDARD SUPPORT SEVERITY 4 Request for information or feature request with no impact on business operations
SUPPORT SERVICE HOURS Live support during customer's choice of time zone.
DATABRICKS STANDARD SUPPORT Limited to break-fix support for the Databricks platform.
DATABRICKS CHAT SUPPORT CHANNEL** Per customer dedicated real-time messaging (e.g., Slack, MSFT Teams) channel available during business hours* for informal communication between the two teams, such as basic questions and information exchange.
MAX NUMBER OF TECHNICAL CONTACTS† The number of technical contacts with access to the Databricks Help Center or Chat Support Channel (if available)
DATABRICKS' SUPPORT FOR SPARK†† Prioritized access to the world's leading Spark technical experts for troubleshooting problems using the product and services.

*Support business hours are Monday through Friday excluding US holidays, from 9AM to 6PM in customer's choice of local North America, Central Europe (CET), Singapore/China (SGT/CST) or Australia Eastern (AET) Timezone.
**Chat Support channel is not covered under the Support SLA response times.
†"Contact" means a unique named user at Customer (whether by email address or Slack ID); accounts may not be shared.
††Additional assistance beyond the original limits can be purchased as consulting services at any time and will be delivered by our professional services team.
If no support is specified in an Order, Customer's support shall be limited to public documentation and forums. **Support is not available to address performance issues on Databricks Jobs Light Compute**

Service Specific Terms

The following Service Specific Terms apply to the specific Databricks Services indicated below. In the event of a conflict or inconsistency between the terms of these Service Specific Terms and the terms of the Databricks Master Cloud Services Agreement or other agreement with us governing your use of the Databricks Services (the "Agreement") the terms and conditions of these Service Specific Terms apply except as noted in Section 1.4 below. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement (or if not therein defined, shall refer to the term in such Agreement that is closest in meaning to such term).

1. **Universal Terms (applicable to all Databricks Services).**

1. Your use of the Platform Services must at all times comply with the Acceptable Use Policy attached hereto.
2. Reserved.
3. If you process the personal data of Authorized End Users or other identifiable individuals in your use of a Databricks Service, you are responsible for providing legally adequate privacy notices and obtaining necessary consents for the processing of such data. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for processing such data in accordance with applicable law.
4. Your use of any Databricks Service described below is subject to these Service Specific Terms notwithstanding anything to the contrary in an Agreement, provided that if your Agreement already contains terms that specifically cover the indicated features below (such terms, "Overriding Terms") (e.g., you entered into the Databricks Master Cloud Services Agreement from 28 March 2022 onwards), the terms in your Agreement will apply and the terms for that specific feature will be considered superseded by your Agreement; if your Agreement limits the applicability of these Service Specific Terms, you are not authorized to enable or access a Databricks Service covered by these Service Specific Terms unless such feature is covered by Overriding Terms.
5. You may perform benchmarks or comparative tests or evaluations (each, a "Benchmark") of the Platform Services and may disclose the results of the Benchmark other than for Beta Services. If you

perform or disclose, or direct or permit any third party to perform or disclose, any Benchmark of any of the Platform Services, you (i) will include in any disclosure, and will disclose to us, all information necessary to replicate such Benchmark, and (ii) agree that we may perform and disclose the results of Benchmarks of your products or services, irrespective of any restrictions on Benchmarks in the terms governing your products or services.

6. Databricks may update the non-material terms from time to time. Updates of the non-material terms shall be deemed effective: (a) for new products and services, upon posting of the updated terms here; and (b) for updates to these terms that were previously posted (i) for Monthly PAYG Service customers (i.e., customers who are not on committed usage contracts), 30 days after such update is made to these Service Specific Terms and notified as described herein or (ii) for all other customers, upon renewal of the applicable Order Form. Databricks will provide notice to anyone who has subscribed to receive an update to these terms as indicated in the introduction above and may additionally provide notice to administrative users of the Platform Services.

2. **Definitions (applicable to all Platform Services).**

1. “Cloud Environment” of a party means the cloud or other compute or storage infrastructure controlled by such party and utilized under the Agreement.
2. “Compute Plane” means the portion of the applicable Cloud Environment where compute resources of the Platform Services are deployed during use of the Platform Services for the primary processing of Customer Data. In the case of Serverless Compute, the Compute Plane is within the Databricks Cloud Environment (the “Databricks Compute Plane”). In all other cases, the Compute Plane is within the Customer Cloud Environment (the “Customer Compute Plane”), and in such cases the processing activity results in fees being charged directly to Customer by the Cloud Service Provider. For the avoidance of doubt, none of the terms “Compute Plane”, “Customer Compute Plane” or “Databricks Compute Plane” include Customer’s cloud storage. In certain Databricks agreements and Documentation, the Compute Plane may be interchangeably referred to as the “Data Plane”.
3. “Databricks Control Plane” means the elements of the Platform Services residing within the Databricks Cloud Environment, other

than the Databricks Compute Plane, including without limitation the user interface of the Platform Services.

4. "Serverless Compute" means a Platform Service where the Compute Plane is located in Databricks' Cloud Environment rather than in Customer's Cloud Environment.

3. **Platform Services - General.**

1. Deployment and Responsibilities.

1. Generally. Customer acknowledges that the Platform Services are implemented in a manner that divides the Platform Services between the Customer Cloud Environment and the Databricks Cloud Environment, and that accordingly each party must undertake certain technical and organizational measures in order to protect the Platform Services and the Customer Content. Without limiting the foregoing, Customer acknowledges and agrees that (1) in order to utilize the current Platform Services other than Serverless Compute, Customer must have an account with the Cloud Service Provider; (2) Databricks does not host the Customer Cloud Environment into which certain parts of the Platform Services may be deployed or the Systems in which your Customer Data may be stored (e.g., an AWS S3 bucket); (3) while certain Customer Data may in some cases be present within the Databricks Cloud Environment of the Platform Services (e.g., within the Customer Results), Databricks' current Platform Services are not designed to archive or permanently retain Customer Data (e.g., they are intended to provide an environment to facilitate Customer's processing of Customer Data by permitting Customer to execute Customer Instructional Input and view Customer Results); and (4) Databricks' current Platform Services do not provide backup services or disaster recovery to enable recovery of Customer Data. Accordingly, and without limiting the foregoing, Databricks is not responsible for any loss, destruction, alteration, or corruption of Customer Content, except to the extent caused by the gross negligence or willful misconduct of Databricks.
2. Your Responsibilities. You acknowledge and agree that you are responsible for (1) protecting the security of all your credentials used to access the Platform Services (with

Databricks also responsible for taking adequate steps to protect Customer credentials to the extent such credentials are within the control of Databricks); (2) securing the Customer Cloud Environment and any Customer System (with such steps to include without limitation the regular rotation of access keys and other industry standard steps to preclude unauthorized access); (3) backing up Customer Instructional Input (e.g., via Github or other third party System); (4) backing up and securing Customer Data under Customer's control within the Customer Cloud Environment or other Customer controlled System (e.g., by turning on versioning and encryption within AWS S3); (5) any security or other issues resulting from any Customer Instructional Input; and (6) managing and paying the charges associated with your usage of the Customer Cloud Environment (e.g., compute and storage fees); and Customer expressly assumes the risks associated with the foregoing responsibilities set forth in this Section.

3. Databricks Responsibilities. Databricks acknowledges and agrees that, as between the parties and except to the extent caused by the action or intentional or negligent inaction of you or your Authorized Users, including without limitation any customizations or configurations of the Platform Services by you or anything specified to be your responsibility above, Databricks is primarily responsible for: (1) the operation (excluding to the extent such operation is directed by the Customer Instructional Input) of the Databricks Cloud Environment (including the user interface of the Platform Services, the Databricks Compute Plane with respect to Serverless Compute, and the portion of the Platform Services within the Databricks Control Plane in which the Customer Instructional Input and Customer Results are held until deleted by you) and, with respect to Platform Services other than Serverless Compute, the Databricks software that operates the computing resources in the Customer Compute Plane; and (2) implementing reasonable technical and organizational measures designed in accordance with ISO/IEC 27001:2013 or equivalent/greater standard to protect the security of the foregoing. Additionally, while it is your responsibility to back up Customer Instructional Input, Databricks will, at your

reasonable request, provide commercially reasonable assistance with recovery efforts where reasonably possible.

2. Platform Services other than Serverless Compute. With respect to your use and Databricks' provisioning of Platform Services other than Serverless Compute, including without limitation All Purpose Compute, Jobs Compute (including Jobs Light Compute) and SQL Compute using Classic SQL Endpoints, the Compute Plane is deployed within the Customer Cloud Environment. Notwithstanding the foregoing, Databricks may in the future add additional Platform Services that may be subject instead to other Service Specific Terms by indicating in the Databricks release notes at the time of release that such Platform Services are subject to additional Service Specific Terms.

Serverless Compute (part of the Platform Services; *in Public Preview on Databricks on AWS as of the date of these Service Specific Terms*). Databricks Serverless Compute, including without limitation Serverless SQL Endpoints, operates by Databricks deploying the Compute Plane into the Databricks Cloud Environment instead of the Customer Cloud Environment. Accordingly, your use of and/or our provision of Databricks Serverless Compute may conflict with or be inconsistent with certain terms you have previously agreed to with Databricks in an Agreement (including without limitation, the terms relating to your deployment or the respective responsibilities of the parties in the terms of service and/or data processing addendum governing the Platform Services, as well as any security schedule or other terms), particularly as such terms may relate to our security obligations or our rights and responsibilities regarding data processing.

3. Unless expressly permitted in an Order Form, Customer may not use Databricks Serverless Compute to process Cardholder Data or PHI.

4. **Downloadable Services**.

1. Databricks may make available to you certain Databricks Services as software from time to time in a downloadable manner ("Downloadable Services"). Unless expressly stated otherwise at the time of download or as otherwise agreed by Databricks,

Downloadable Services may only be used as a part of the Databricks Services. You are granted a non-exclusive, royalty-free right and license to use and copy during the term of the Agreement the Downloadable Services solely as necessary to enable your use of the Databricks Services.

5. **Beta Services.**

1. "Beta Service" means any Databricks Service (or feature of a Databricks Service) that is clearly designated as "beta", "experimental", "preview" or similar, that is provided prior to general commercial release, and that Databricks at its sole discretion offers to Customer, and Customer at its sole discretion elects to use.
2. If you elect to receive any Beta Services offered by Databricks, you agree that, in addition to adhering to all other restrictions generally applicable to your use of the Platform Services under the Agreement and any requirements set forth by Databricks in writing regarding the particular Beta Services, you will not use such Beta Services for production workloads or for any mission critical work, and that you will not use sensitive data (e.g., PHI or Cardholder Data) in conjunction with such Beta Services unless explicitly permitted in an Order Form. For the avoidance of doubt, information pertaining to the Beta Services constitutes Databricks Confidential Information.
3. BETA SERVICES ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND. CUSTOMER BEARS THE RISK OF USING THE BETA SERVICES. DATABRICKS AND ITS SUPPLIERS GIVE NO EXPRESS OR IMPLIED WARRANTIES, GUARANTEES OR CONDITIONS RELATED TO THE BETA SERVICES. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, DATABRICKS AND ITS SUPPLIERS EXCLUDE THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

6. **Databricks Container Services (part of the Platform Services).**

1. As part of the Databricks Container Services, Databricks may provide a sample stub container file (a "Sample Container") that you may (but are not required to) use to create a custom container file to use with Databricks Container Services (a

"Modified Sample Container"). Databricks grants you a limited, non-exclusive right and license to use and modify the Sample Container by inserting your own code into the Sample Container to create a Modified Sample Container. The Sample Container may contain libraries that are subject to open source licenses. It is your obligation to review and comply with any such licenses prior to the creation of the Modified Sample Container.

2. You may not:

    1. upload to the Platform Services or otherwise make available for use with Databricks Services a container file (including a Modified Sample Container) (together, a "Custom Container") or other code that contains any viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs designed to impede the use of the Databricks Services or any other systems, whether or not connected to the Databricks Services;
    2. include in a Custom Container any code for which you do not have the necessary right or license or that contains any code that could subject Databricks Services (including the Databricks Container Services) to any term that seeks to require Databricks to make any Databricks Services code available in source code form or which may impose any other obligation or restriction with respect to Databricks' intellectual property rights; or
    3. attempt to disable or interfere with any technical limitations contained within Databricks Container Services.

3. You grant Databricks a worldwide, non-exclusive royalty free right and license to use, reproduce and make derivative works of the Custom Container solely as necessary to provide Databricks Container Services.

7. **Delta Sharing (part of the Platform Services; in Preview on Databricks on AWS as of the date of these Service Specific Terms).**

    1. Delta Sharing allows a Databricks Authorized User to share data outside of the Authorized User's Customer organization. Accordingly, Customer's use of and/or Databricks' provision of Delta Sharing may conflict with or be inconsistent with certain terms you have previously agreed to with Databricks in an Agreement (including, without limitation, terms relating to your

deployment or the respective responsibilities of the parties in the terms of service and/or data processing addendum governing the Platform Services, as well as any security schedule or other terms), particularly as such terms may relate to our security obligations or our rights and responsibilities regarding data processing.

2. Additional Terms Relating to your Deployment.

1. Additional Definitions. The following additional terms apply to any use of Delta Sharing (as defined below).

1. "Data Recipient" means a person who receives Customer Data from a Data Provider through Delta Sharing. A Data Recipient may be another Databricks customer or may be a third party entity that is not a Databricks customer ("Non-Customer Recipient").
2. "Data Share" means an individual set of Shared Data.
3. "Data Provider" means a person who initiates the share of the Customer Data from the Platform Services.
4. "Delta Sharing" means the portion of the Databricks Platform Services that enable a Data Provider to share Customer Data with a Data Recipient, as further described in the Documentation.
5. "Shared Data" means Customer Data (either Customer's Customer Data or the Customer Data of another Databricks customer) that is shared via Delta Sharing.

2. Generally. The Platform Services include functionality that lets Customer, at its option and in its sole discretion, provide Data Recipients outside of its Databricks workspace(s) with read-only access to Shared Data or receive Shared Data from other Data Providers.
3. When Customer is the Data Provider. Customer may, at its option and in its sole discretion and subject to the rest of the Agreement, use Delta Sharing to grant one or more Data Recipients read-only access to some or all of its Customer Data via one or more Data Shares. Customer:

1. is solely responsible for ensuring that it is entitled to share any Shared Data with any Recipient and that any such Data Share is in compliance with all applicable laws.
2. acknowledges and agrees that (i) Data Recipients will have ongoing access to the Shared Data with the permissions set by Customer until the applicable Data Share is disabled; (ii) nothing in Delta Sharing prevents a Data Recipient from making a permanent copy of the Shared Data; (iii) Databricks has no control over, and will have no liability for, the acts or omissions of any Data Recipient with respect to the Shared Data; and (iv) Customer remains responsible for all Customer Data in accordance with the Agreement, irrespective of whether Customer or Data Recipient is in control of such data.
3. as between Databricks and Customer, acknowledges and agrees that it is responsible for any fees (including fees charged by a Cloud Service Provider) associated with the access to and use of any Shared Data by a Data Recipient.
4. represents that it has the right to share with Databricks any personal data associated with any Data Recipients that it shares with Databricks.
5. acknowledges and agrees that it is fully responsible for any actions or inactions of a Data Recipient with respect to the Shared Data. When Customer is the Data Recipient. By accessing a Data Provider's Shared Data as a Data Recipient, Customer represents that it has been authorized to access the Data Share(s) provided to it by the Data Provider and acknowledges that (1) Databricks has no liability for such Shared Data or Customer's use of such Shared Data, and (2) Databricks may collect information about Customer's use of and access to the Shared Data (including identifying Customer and any individual who accesses the Shared Data using the credential file in connection with such information) and may share it with the applicable Data Provider.

3. Restrictions on Shared Data; Suspension. Unless set forth in an Order Form, Customer may not include any PHI (as defined by the Health Insurance Portability and Accountability Act) or Cardholder Data (as defined by PCI-DSS) in any Shared Data. Customer acknowledges and agrees that Databricks may, but is not required to, disable a given Data Share or Customer's use of the Delta Sharing or access to a Data Share if Databricks reasonably suspects or becomes aware of a claim that a Data Share may violate applicable law or may harm Databricks, Customer, Recipient or other third party.

Security Addendum

This Security Addendum is incorporated into and made a part of the written agreement between Databricks, Inc. ("**Databricks**") and Customer that references this Security Addendum ("**Agreement**"). Databricks maintains a comprehensive documented security program that is based on industry standard security frameworks including ISO 27001 and ISO 27018 (the "**Security Program**"). Pursuant to the Security Program, Databricks implements and maintains administrative, physical, and technical security measures to protect the Platform Services and Support Services and the security and confidentiality of Customer Content (including any Customer Personal Data that may be contained therein) (each as defined in the Agreement) under Databricks' control that is processed by Databricks in its provisioning of the Platform Services or Support Services (the "**Security Measures**"). Databricks' compliance with this Addendum shall be deemed to satisfy any more general measures included within any Agreement, including the Service Specific Terms. In accordance with its Security Program, Databricks will, when any Customer Content is under its control: (i) comply with the Security Measures identified below with respect to such Customer Content, and (ii) where relevant, keep documentation of such Security Measures. Databricks regularly tests and evaluates its Security Program, and may review and update this Security Addendum at any time without notice, provided that such updates are equivalent (or enhance) security and do not materially diminish the level of protection afforded to Customer Content by these Security Measures.

1. **Deployment Model**

    1. **Shared Responsibility**. Databricks operates in a shared responsibility model, where both Databricks and the Customer maintain security responsibilities. This is covered in more detail in our Documentation.
    2. **Architecture**. Databricks is a hybrid platform-as-a-service offering. The components responsible for managing and controlling the Platform Services are referred to as the 'Databricks Control Plane' and are hosted within a Databricks Cloud Service Provider account. The compute resources that perform data processing operations are referred to as the "Data Plane". For certain Cloud Service Providers, the Data Plane may either be deployed in the Customer's Cloud Service Provider account

(known as the 'Customer Data Plane') or, for Databricks Serverless Compute, in a Databricks-controlled Cloud Service Provider account (known as the 'Databricks Data Plane'). Data Plane shall refer to both Customer Data Plane and Databricks Data Plane unless otherwise specified.

3. **Compute Resources**. Compute resources are created and coordinated by the Databricks Control Plane and deployed into the Data Plane. Compute resources are launched as new virtual machines that leverage the latest base image and Databricks source code and do not have data from previous machines. When compute resources terminate, the data on their local hard drives is overwritten by Databricks or by the Cloud Service Provider.
4. **Data Storage of Customer Content**.
    1. **Customer Data and Customer Results**.
        1. **Customer Control**. Most Customer Data is stored within the Customer's own Cloud Service Provider account at rest (e.g., within Customer's AWS S3 bucket) or within other Systems under Customer's control. Customer may choose where this Customer Data resides (other than the DBFS root, which is deployed into a storage bucket within the applicable Cloud Service Provider in the region in which the Data Plane is deployed). Please see the Documentation for more details.
        2. **Databricks Control**. Small amounts of Customer Data may be stored within the Databricks Control Plane, including Customer Results and metadata about Customer Data (e.g., contained within the metastore). Databricks offers Customers options regarding the storage of certain Customer Content within the Platform Services (e.g., the location of Customer Results created by the use of interactive notebooks). Please see the Documentation for more details.
    2. **Customer Instructional Input**. Customer Instructional Input is stored at rest within the Databricks Control Plane.
2. **Deployment Region**. Customers may specify the region(s) where their Platform Services Workspaces are deployed. Customers can choose to

deploy the Data Plane into any supported Databricks region. The Databricks Control Plane is deployed into the same region. Databricks will not, without Customers' permission, move a Customer Workspace into a different region. See the Documentation for details specific to Customer's Cloud Service Provider.

3. **Databricks' Audits & Certifications**. Databricks uses independent third-party auditors to assess the Databricks Security Program at least annually, as described in the following audits, regulatory standards, and certifications:

    1. SOC 2 Type II (report available under NDA)
    2. ISO 27001
    3. ISO 27018
    4. HIPAA (AWS, for HIPAA-compliant deployments)
    5. PCI DSS (AWS, for PCI-compliant deployments)

4. **Administrative Controls**

    1. **Governance**. Databricks' Chief Security Officer leads the Databricks' Information Security Program and develops, reviews, and approves (together with other stakeholders, such as Legal, Human Resources, Finance, and Engineering) Databricks' Security Policies (as defined below).
    2. **Change Management**. Databricks maintains a documented change management policy, reviewed annually, which includes but is not limited to, evaluating changes of or relating to systems authentication.
    3. **ISMS; Policies and Procedures.** Databricks has implemented a formal Information Security Management System ("**ISMS**") in order to protect the confidentiality, integrity, authenticity, and availability of Databricks' data and information systems, and to ensure the effectiveness of security controls over data and information systems that support operations. The Databricks Security Program implemented under the ISMS includes a comprehensive set of privacy and security policies and procedures developed and maintained by the security, legal, privacy, and information security teams ("**Security Policies**"). The Security Policies are aligned with information security standards (such as ISO 27001) and cover topics including but not limited to: security controls when accessing Customer Workspaces; confidentiality of Customer Content; acceptable use of company

technology, systems and data; processes for reporting security incidents; and privacy and security best practices. The Security Policies are reviewed and updated annually.

4. **Personnel Training.** Personnel receive comprehensive training on the Security Policies upon hire and refresher trainings are given annually. Personnel are required to certify and agree to the Security Policies and personnel who violate the Security Policies are subject to disciplinary action, including warnings, suspension and up to (and including) termination.
5. **Personnel Screening and Evaluation**. All personnel undergo background checks prior to onboarding (as permitted by local law), which may include, but are not limited to, criminal record checks, employment history verification, education verification, and global sanctions and enforcement checks. Databricks uses a third-party provider to conduct screenings, which vary by jurisdiction and comply with applicable local law. Personnel are required to sign confidentiality agreements.
6. **Monitoring & Logging**. Databricks employs monitoring and logging technology to help detect and prevent unauthorized access attempts to its network and equipment.
7. **Access Review**. Active users with access to the Platform Services are reviewed at least quarterly and are promptly removed upon termination of employment. As part of the personnel offboarding process, all accesses are revoked and data assets are securely wiped.
8. **Third Party Risk Management**. Databricks assesses the security compliance of applicable third parties, including vendors and subprocessors, in order to measure and manage risk. This includes, but is not limited to, conducting a security risk assessment and due diligence prior to engagement and reviewing external audit reports from critical vendors at least annually. In addition, applicable vendors and subprocessors are required to sign a data processing agreement that includes compliance with applicable data protection laws, as well as confidentiality requirements.

5. Physical and Environmental Controls

1. **Databricks Corporate Offices.** Databricks has implemented administrative, physical, and technical safeguards for its corporate offices. These include, but are not limited to, the below:

1. Visitors are required to sign in, acknowledge and accept an NDA, wear an identification badge, and be escorted by Databricks personnel while on premises
2. Databricks personnel badge into the offices
3. Badges are not shared or loaned to others without authorization
4. Physical entry points to office premises are recorded by CCTV and have an access card verification system at every door, allowing only authorized employees to enter the office premises
5. Equipment and other Databricks-issued assets are inventoried and tracked
6. Office Wi-Fi networks are protected with encryption, wireless rogue detection, and Network Access Control

2. **Cloud Service Provider Data Centers**. Databricks regularly reviews Cloud Service Provider audits conducted in compliance with ISO 27001, SOC 1, SOC 2, and PCI-DSS. Security controls include, but are not limited to the list below:

1. Biometric facility access controls
2. Visitor facility access policies and procedures
3. 24-hour armed physical security
4. CCTV at ingress and egress
5. Intrusion detection
6. Business continuity and disaster recovery plans
7. Smoke detection sensors and fire suppression equipment
8. Mechanisms to control temperature, humidity and water leaks
9. Power redundancy with backup power supply

Systems & Network Security

0. **Platform Controls**.

1. **Isolation**. Databricks leverages multiple layers of network security controls, including network-level isolation, for separation between the Databricks Control Plane and Customer Data Plane, and between Workspaces within the Databricks Data Plane. See documentation on Serverless

Compute for more details on the difference between Serverless Compute and non-Serverless Compute.

2. **Firewalls & Security Groups**. Firewalls are implemented as network access control lists or security groups within the Cloud Service Provider's account. Databricks also configures local firewalls or security groups within the Customer Data Plane.
3. **Hardening.**

    1. Databricks employs industry standards to harden images and operating systems under its control that are deployed within the Platform Services, including deploying baseline images with hardened security configuration such as disabled remote root login, isolation of user code, and images are regularly updated and refreshed.
    2. For Systems under Databricks control supporting the production data processing environment, Databricks tracks security configurations against industry standard baselines such as CIS and STIG.

4. **Encryption**

    1. **Encryption of data-in-transit**. Customer Content is encrypted using cryptographically secure protocols (TLS v.1.2 or higher) in transit between (1) Customer and the Databricks Control Plane and (2) the Databricks Control Plane and the Data Plane. Additionally, depending on functionality provided by the Cloud Service Provider, Customers may optionally encrypt communications between clusters within the Data Plane (e.g., by utilizing appropriate AWS Nitro instances).
    2. **Encryption of data-at-rest**. Customer Content is encrypted using cryptographically secure protocols (AES-128 bit, or the equivalent or better) while at rest within the Databricks Control Plane. Additionally, depending on functionality provided by the Cloud Service Provider, Customers may optionally encrypt at rest Customer Content within the Data Plane. See Documentation on ‘local disk encryption’ for more details.

3. **Review**. Cryptographic standards are periodically reviewed and selected technologies and ciphers are updated in accordance with assessed risk and market acceptance of new standards.
4. **Customer Options; Responsibilities**. Customers may choose to leverage additional encryption options for data in transit within the Customer Data Plane or Databricks Data Plane as described in the Documentation (e.g., Customer may utilize AWS Nitro EC2 instances within the Customer Data Plane to provide additional encryption in transit). Customer shall, based on the sensitivity of the Customer Content, configure the Platform Services and Customer Systems to encrypt Customer Content where appropriate (e.g., by enabling encryption at rest for data stored within AWS S3).

5. **Monitoring & Logging**

    1. **Intrusion Detection Systems**. Databricks leverages security capabilities provided natively by Cloud Service Providers for security detection.
    2. **Audit Logs**.

        1. **Generation**. Databricks generates audit logs from Customer's use of the Platform Services. The logs are designed to store information about material events within the Platform Services.
        2. **Delivery**. Customer may, depending on the entitlement tier of the Platform Services, enable delivery of audit logs. It is Customer's responsibility to configure this option.
        3. **Integrity**. Databricks stores audit logs in a manner designed to protect the audit logs from tampering.
        4. **Retention**. Databricks stores audit logs for at least one year.

6. **Penetration Testing**. Databricks conducts third-party penetration tests at least annually, employs in-house

offensive security personnel, and also maintains a public bug bounty program.

7. **Vulnerability Management & Remediation**. Databricks regularly runs authenticated scans against representative hosts in the SDLC pipeline to identify vulnerabilities and emerging security threats that may impact the Data Plane and Databricks Control Plane. Databricks will use commercially reasonable efforts to address critical vulnerabilities within 14 days, high severity within 30 days, and medium severity within 60 days measured from, with respect to publicly declared third party vulnerabilities, the date of availability of a compatible, vendor-supplied patch, or for internal vulnerabilities, from the date such vulnerability is confirmed. Databricks leverages the National Vulnerability Database's Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating, combined with an internal analysis of contextual risk to determine criticality.
8. **Patching**.
    1. **Control Plane**. Databricks deploys new code to the Databricks Control on an ongoing basis.
    2. **Data Plane**. New Data Plane virtual machines use the latest applicable source code and system images upon launch and do not require Databricks to patch live systems. Customers are encouraged to restart always-on clusters on a periodic basis to take advantage of security patches.
9. **Databricks Personnel Login to Customer Workspaces**. Databricks utilizes an internal technical and organizational control tool called 'Genie' that permits Databricks personnel to log in to a Customer Workspace to provide support to our Customers and permits limited Databricks engineering personnel to log in to certain Platform Services infrastructure. Customer may optionally configure certain limitations on the ability for Databricks personnel to access Customer Workspaces. Please see Documentation on 'Genie' for more details, including on which Cloud Service Providers this is offered.

1. **Corporate Controls.**

1. **Access Controls**
    1. **Authentication**. Databricks personnel are authenticated through single sign-on (SSO), 802.1x (or similar) where applicable, and use a unique user ID and password combination and multi-factor authentication. Privileges are consistent with least privilege principles. Security Policies prohibits personnel from sharing or reusing credentials, passwords, IDs, or other authentication information. If your identity provider supports the SAML 2.0 protocol, you can use Databricks' SSO to integrate with your identity provider.
    2. **Role-Based Access Controls (RBACs).** Only authorized roles are allowed to access systems processing customer and personal data. Databricks enforces RBACs (based on security groups and access control lists), and restricts access to Customer Content based on the principle of 'least privilege' and segregation of responsibilities and duties.
2. **Pseudonymization**. Information stored in activity logs and databases are protected where appropriate using a unique randomized user identifier to mitigate risk of re-identification of data subjects.
3. **Workstation Controls**: Databricks enforces certain security controls on its workstations used by personnel, including:
    1. Full-disk encryption
    2. Anti-malware software
    3. Automatic screen lock after 15 minutes of inactivity
    4. Secure VPN

Incident Detection & Response

0. **Detection & Investigation**. Databricks' dedicated Detection engineering team deploys and develops intrusion detection monitoring across its computing resources, with alert notifications sent to the Security Incident Response Team (SIRT) for triage and response. The SIRT employs an incident response framework to manage and minimize the effects of unplanned security events.

1. **Security Incidents; Security Breaches**. “Security Breach” means a breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data under Databricks control. A “Security Incident” is any actual or attempted breach of security that does not rise to the level of a Security Breach. A Security Breach shall not include an unsuccessful attempt or activity that does not compromise the security of Customer Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents. Databricks maintains a record of known Security Incidents and Security Breaches that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed Security Incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed Security Incidents, Databricks will take appropriate, reasonable steps to minimize product and Customer damage or unauthorized disclosure. All incidents are logged in an incident tracking system that is subject to auditing on an annual basis.
2. **Communications & Cooperation**. In accordance with applicable data protection laws, Databricks will notify Customer of a Security Breach for which that Customer is impacted without undue delay after becoming aware of the Security Breach, and take appropriate measures to address the Security Breach, including measures to mitigate any adverse effects resulting from the Security Breach.

Backups, Business Continuity, and Disaster Recovery

0. **Business Continuity and Disaster Recovery.** Databricks Business Continuity (BC) and Disaster Recovery (DR) plans are reviewed and drills are conducted annually.
1. **Data Resiliency.** Databricks performs backups for the Databricks Control Plane (including any Customer Instructional Input stored therein), generally managed by the Cloud Service Provider capabilities, for data resiliency purposes in the case of a critical systems failure. While Databricks backs up Customer notebooks that persist in the Databricks Control Plane as part of its systems resiliency, those backups are maintained only for emergency

recovery purposes and are not available for Customers to use on request for recovery purposes.

2. **No Data Restoration.** Due to the hybrid nature of the Databricks Platform, Databricks does not provide backup for Customer Content, and Databricks is unable to restore an individual Customer's Instructional Input upon request. To assist Customers in backing up Customer Instructional Input, Databricks provides certain features within the Platform Services (like the ability to synchronize notebooks via a customer's Github or Bitbucket account).
3. **Self-service Access.** Databricks makes available certain features within the Platform Services that permit customers to access, export and delete certain Customer Content (e.g., notebooks) contained within the Databricks Control Plane. Please see the Documentation related to 'manage workspace storage'.
4. **Customer Managed Backups.** Customers retain ownership of their Customer Content and must manage their own backups, including to the extent applicable, enabling backup within the Systems in which the Customer Data is stored.

Data Deletion.

0. **During Use**. The Platform Services provide Customers with functionality that permit Customers to delete Customer Content under Databricks' control.
1. **Upon Workspace Cancellation**. Customer Content contained within a Customer Workspace is permanently deleted within thirty (30) days following cancellation of the Workspace.

Secure Software Development Lifecycle ("SDLC")

0. **Security Champions**. Databricks Engineering and the security organization co-run a Security Champions program, in which senior engineers are trained and socialized as virtual members of the security team. Security Champions are available to all engineering staff for design or code review.
1. **Security Design Review**. Feature designs are assessed by security personnel for their security impact to the Databricks Platform, for example, additions or modifications to access controls, data flows, and logging.

2. **Security Training**. Engineers are required to take Secure SDLC training, including but not limited to, content provided by OWASP.
3. **Peer Code Review**. All production code must be approved through a peer code review process.
4. **Change Control.** Databricks' controls are designed to securely manage assets, configurations, and changes throughout the SDLC.
5. **Code Scanning**. Static and dynamic code scans are regularly run and reviewed.
6. **Penetration Testing**. As part of the Security Design Review process, certain features are identified and subjected to penetration testing prior to release.
7. **Code Approval**. Functional owners are required to approve code in their area of responsibility prior to the code being merged for production.
8. **Multi-Factor Authentication**. Accessing the Databricks code repository requires Multi-Factor Authentication.
9. **Code Deployment**. Production code is deployed via automated continuous integration / continuous deployment (CI/CD) pipeline processes. The release management teams are separated from the engineering teams that build the product.
10. **Production Separation**. Databricks separates production Platform Services Systems from testing and development Platform Services Systems.

Acceptable Use Policy – Paid (Including Trial)

For the paid (including trial) version of Databricks

This Databricks acceptable use policy ("**AUP**") sets forth certain restrictions relating to the access to, and use of, the Databricks Services by you or someone on your behalf under your agreement with Databricks applicable to the Databricks Services ("**Agreement**"). The restrictions set forth in this AUP are not exhaustive. Any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. The non-material restrictions of this AUP may be updated by Databricks from time to time upon reasonable notice, which may be provided through the Databricks Services or by posting an updated version of this AUP. Updates of the AUP become binding, including on existing users, on the later of the date specified in the updated AUP or thirty (30) days after posting. Any modification to the AUP within an update will relate solely to restrictions on use of, and access to, the Databricks Services. In accordance with General Services Administration Acquisition Regulation (GSAR) 552.212-4(w)(1)(iv) Continued Performance, and violation of this AUP may result in the suspension or termination of your access to and use of the Databricks Services.

You shall not (and shall not permit your Authorized Users to):

1. attempt to access, search, or create accounts for any of our services by any means other than our publicly supported interfaces or as otherwise authorized by us;
2. create multiple accounts for the purpose of extending your free trial;
3. interfere with or disrupt (or attempt to interfere with or disrupt) the Databricks Services, or gain (or attempt to gain) access to any Systems that connect thereto (except as required to appropriately access and use the Databricks Services);
4. use the Databricks Services to violate the security or integrity of, or otherwise abuse, any System of any party (including without limitation the Platform Services or Support Services), including but not limited to gaining unauthorized access to any System (including attempting to

probe, scan, monitor, or test the vulnerability of a System), forging any headers or other parts of any message describing its origin or routing, interfering with the proper functioning of any System (including any deliberate attempt by any means to overload a System), implementing denial-of-service attacks, operating non-permissioned network services (including open proxies, mail relays or recursive domain name servers), using any means to bypass System usage limitations, or storing, transmitting or installing malicious code;

5. use the Databricks Services to distribute or facilitate the sending of unsolicited or unlawful (i) email or other messages, or (ii) promotions of any kind;
6. use the Databricks Services to engage in or promote any other fraudulent, deceptive or illegal activities;
7. use the Databricks Services to process, store or transmit material, including any Customer Data, in violation of any Law or any third party rights, including without limitation privacy rights;
8. provide a custom deployment name for your Workspace that might reasonably be considered inappropriate or that includes the trade name of any third party unless such party has provided you with express writing permission;
9. disclose any benchmarking of the Databricks Services except as set forth in the Service Specific Terms; or
10. use the Databricks Services in any circumstances where failure could lead to death, personal injury or environmental damage, and you further acknowledge that the Databricks Services are not designed or intended for such use.

Databricks may modify custom deployment names if they are found to be in violation of this AUP.

Inactive Monthly PAYG accounts:

If an account for which Databricks is providing Monthly PAYG Services is found to be inactive, the account may be suspended or terminated by Databricks, and any Customer Content relating to such account that is stored within the Subscription Services or other Databricks Systems may be deleted. Databricks will provide at least 30 days' notice (in accordance with the Agreement) prior to permanently deleting your account, unless we deem it reasonably necessary to suspend or terminate your account without notice. For the avoidance of doubt, if we determine that the email associated with

your account is invalid (e.g., because it bounces upon our notification of inactivity), we may terminate your account without further notice.

An account may be considered inactive if:

- No Customer Authorized User has logged into the account for at least six months;
- No Customer Instructional Input was ever created within or input into the account and at least three months has passed since the account was established; or
- If your account is set up to be paid by credit card, you (i) did not provide a valid credit card number or (ii) you failed to update an expired or invalid credit card number and at least three months has passed without a valid credit card number being on file, provided that for the avoidance of doubt this provision does not limit Databricks' right to terminate your account for non-payment relating to actual usage.

DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Annexes and the Standard Contractual Clauses ("**DPA**"), forms an integral part of the Databricks Master Cloud Services Agreement, or any other written agreement that governs Customer's use of the Databricks Services (as defined below) entered into between the entity identified as the "Customer" in the signature block below ("**Customer**") and Databricks, Inc. ("**Databricks**") (the "**Agreement**"), and applies solely to the extent that Databricks processes any Personal Data (defined below) in connection with the Databricks Services. By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. For the purposes of the DPA only, and except where otherwise indicated, the term "Customer" shall include Customer and its Authorized Affiliates.

1. DEFINITIONS

1.1. **"Applicable Data Protection Laws"** means all data protection and privacy laws and regulations applicable to the processing of Personal Data under the Agreement, including (where applicable) European Data Protection Laws and the CCPA.

1.2. **"Authorized Affiliate"** means a Customer Affiliate who is authorized to use the Databricks Services under the Agreement and who has not signed their own separate "Agreement" with Databricks.

1.3. **"CCPA"** means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, *et seq.)*, as may be amended, superseded or replaced from time to time.

1.4. "**Customer Content"** means, if not defined within the Agreement, all data input into or made available by Customer for processing within the Databricks Services or generated from the Databricks Services.

1.5. **"Databricks Services"** means the Platform Services and/or any other services (e.g. Advisory or Support Services) provided directly by Databricks to Customers under the Agreement.

1.6. **"European Data Protection Laws"** means (a) Regulation 2016/679 (General Data Protection Regulation) ("**EU GDPR**"); (b) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss Data Protection Act**"); in each case as may be amended, superseded or replaced from time to time.

1.7. **"Personal Data"** means any 'personal data' or 'personal information' contained within Customer Content or provided to Databricks for processing under the Agreement by or on behalf of Customer in the provision of the Databricks Services.

1.8. **"Restricted Transfer"** means a transfer (directly or via onward transfer) of personal data that is subject to European Data Protection Laws to a third country outside the European Economic Area, United Kingdom and Switzerland which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).

1.9. **"Security Addendum"** means the security addendum found at Databricks.com/legal/security-addendum.

1.10. **"Security Breach"** means a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.11. **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded or replaced from time to time.

1.12. **"Subprocessor"** means any other processor engaged by Databricks (including any Databricks Affiliate) to process Personal Data.

1.13. **"UK Addendum"** means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioners Office under S.119 (a) of the UK Data Protection Act 2018, as updated or amended from time to time.

1.14. The terms **"controller"**, **"data subject"**, **"supervisory authority"**, **"processor"**, **"process"**, **"processing"**, **"personal data"**, and **"personal information"** shall have the meanings given to them in Applicable Data Protection Laws. The term "controller" includes "business", the term "data subject" includes "consumers", and the term "processor" includes "service provider" (in each case, as defined by the CCPA).

2. PROCESSING OF PERSONAL DATA

2.1. **Scope and Roles of the Parties.** This DPA applies when Personal Data is processed by Databricks as a processor or subprocessor in its provision of the Databricks Services to Customer, who will act as either a controller or processor of Personal Data.

2.2. **Customer Processing.** Customer shall have sole responsibility for the accuracy and quality of Personal Data, and for providing any notices and obtaining any consents, permissions and rights required to enable Databricks to process Personal Data. Customer shall ensure that its instructions and processing of Personal Data comply with Applicable Data Protection Laws.

2.3. **Databricks Processing.** Databricks shall process Personal Data only in accordance with Customer's documented lawful instructions. For these purposes, Customer instructs Databricks to process Personal Data for the following purposes: (a) processing in accordance with the Agreement and any applicable Order Form(s); (b) processing initiated by Customer and Authorized Users in their use or configuration of the Databricks Services; and (c) processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement. Databricks is not responsible for determining if Customer's instructions are compliant with applicable law. However, Databricks shall notify Customer in writing if, in its reasonable opinion, the Customer's processing instructions infringe Applicable Data Protection Laws and provided that Customer acknowledges that Personal Data may be processed on an automated basis in accordance with Customers' use of the Databricks Services, which Databricks does not monitor.

2.4. **Details of Processing.** The details of the processing of Personal Data by Databricks are set out in Annex A to the DPA.

3. CONFIDENTIALITY

3.1. **Personnel.** Databricks shall ensure that any employees or personnel it authorizes to process Personal Data is subject to an appropriate duty of confidentiality.

4. SUBPROCESSING

4.1. **Authorization.** Customer provides a general authorization to Databricks use of Subprocessors to process Personal Data in accordance with this Section, including those Subprocessors listed at www.Databricks.com/subprocessors ("**Subprocessor List**").

4.2. **Subprocessor Obligations.** Databricks shall (i) enter into a written agreement with its Subprocessors, which includes data protection and security measures no less protective of Personal Data than the Agreement and this DPA; and (ii) remain fully liable for any breach of the Agreement and this DPA that is caused by an act, error or omission of its Subprocessors to the extent that Databricks would have been liable for such act, error or omission had it been caused by Databricks.

4.3. **Subprocessor Changes.** At least thirty (30) calendar days prior to the date on which any new Subprocessor shall commence processing Personal Data, Databricks shall update the Subprocessor List and provide Customer with notice of that update. Such notice will be sent to individuals who have

signed up to receive updates to the Subprocessor List via the mechanism(s) indicated on the Subprocessor List.

4.4. **Subprocessor Objections.** Customer may object to Databricks' appointment of a new Subprocessor on reasonable grounds relating to data protection by notifying Databricks in writing at privacy@databricks.com within ten (10) calendar days after receiving notice pursuant to Section 4.3. In such event, Databricks shall either: (a) work with Customer to address Customer's objections to its reasonable satisfaction; (b) instruct the Subprocessor to not process Personal Data; or (c) notify Customer of its option to terminate the Agreement and this DPA within fourteen (14) calendar days. If Customer exercises its right to terminate the Agreement and this DPA, Databricks will provide Customer with a pro rata reimbursement of any prepaid, but unused fees.

5. ASSISTANCE

5.1. **Data Subject Requests.** Customer is responsible for responding to and complying with data subject requests ("**DSR**"). The Databricks Services include controls that Customer may use to assist it to respond to DSR. If Customer is unable to access or delete any Personal Data using such controls, Databricks shall, taking into account the nature of the processing, reasonably cooperate with Customer to enable Customer to respond to the DSR. If a data subject sends a DSR to Databricks directly and where Customer is identified or identifiable from the request, Databricks will promptly forward such DSR to Customer and Databricks shall not, unless legally compelled to do so, respond directly to the data subject except to refer them to the Customer to allow Customer to respond as appropriate.

5.2. **Data Protection Impact Assessments**. Databricks will provide commercially reasonable assistance to Customer (at Customer's expense) with respect to any legally required data protection impact assessment relating to the processing or proposed processing of Personal Data in connection with the Databricks Services and any related required consultation with supervisory authorities.

5.3. **Legal Requests.** If Databricks receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Personal Data, Databricks will attempt to redirect the governmental body to request such Personal Data directly from Customer. As part of this effort, Databricks may provide Customer's basic contact information to the governmental body. If compelled to disclose Personal Data to a governmental body, then Databricks will give Customer reasonable notice of the legal demand to allow Customer to seek a protective order or other appropriate remedy, unless Databricks is legally prohibited from doing so.

6. SECURITY

6.1. **Security Measures.** Databricks has implemented and will maintain appropriate technical and organizational security measures as set forth in the Security Addendum ("**Security Measures**"). The Security Measures are subject to technical progress and development and Databricks may update the Security Measures, provided that any updates shall not materially diminish the overall security of Personal Data or the Databricks Services. Databricks may make available certain security controls within the Databricks Services that Customer may use in accordance with the Documentation.

6.2. **Security Breach Notification.** In the event of a Security Breach, Databricks will (a) notify Customer in writing without undue delay and in no event later than seventy-two (72) hours after becoming aware of the Security Breach; and (b) promptly take reasonable steps to contain, investigate, and mitigate any adverse effects resulting from the Security Breach. Databricks will reasonably cooperate with and assist Customer with respect to any required notification to supervisory authorities or data subjects (as applicable), taking into account the nature of the processing, the information available to Databricks, and any restrictions on disclosing the information (such as confidentiality).

7. AUDITS AND RECORDS

7.1. **Audit Program.** Databricks uses external auditors to verify the adequacy of its security measures with respect to its processing of Personal Data. Such audits are performed (a) at least once annually; (b) according to ISO 27001 standards or such other alternative standards that are substantially equivalent

to ISO 27001; and (c) by independent third party security professionals selected by Databricks. Such audits result in the generation of a confidential audit report ("**Audit Report**").

7.2. **Audit Report.** At Customer's written request, and no more than once every twelve (12) months, Databricks will provide Customer with a copy of the Audit Report so that Customer can verify Databricks' compliance with this DPA. The Audit Report shall be considered Databricks' confidential information and subject to the confidentiality provisions of the Agreement. To the extent that the Audit Report is deemed insufficient by a supervisory authority, Customer may request an on-site audit, subject to the additional terms in Section 7.3.

7.3. **Onsite Audit**. An on-site audit shall be conducted by Customer (a) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Databricks Services used by Customer; (b) up to one time per year with at least three weeks' advance written notice; and (c) during Databricks normal business hours, under reasonable duration and shall not unreasonably interfere with Databricks' day-to-day operations. Further, before any on-site audit commences, Customer and Databricks shall mutually agree upon the scope, timing, duration of the audit and costs for which Customer shall be responsible.

8. TRANSFER OF PERSONAL DATA

8.1. **Restricted Transfers.** Where the transfer of Personal Data to Databricks is a Restricted Transfer, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form an integral part of the Agreement in accordance with Annex B of this DPA.

8.2. **Alternative Transfer Mechanisms**. If and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Personal Data to Databricks, the parties shall reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Personal Data. Additionally, in the event Databricks adopts an alternative transfer mechanism (including any successor version of the Privacy Shield), such alternative transfer mechanism shall apply instead of the SCCs described in Section 8.1 of this DPA (but only to the extent such alternative transfer mechanism complies with applicable European Data Protection Laws and extends to the territories to which Personal Data is transferred).

9. BACKUP, DELETION & RETURN

9.1. **No Backups.** The Databricks Services do not include backup services or disaster recovery for Personal Data. Databricks does provide functionality within the Databricks Services that may permit Customer to backup certain Personal Data on its own. It is the Customer's obligation to backup any Personal Data if desired.

9.2. **Deletion.** The Databricks Services include controls that Customer may use at any time during the term of the Agreement to retrieve or delete Personal Data. Subject to the terms of the Agreement, Databricks will delete Personal Data from the Databricks Services when Customer uses such controls to send an instruction to delete.

9.3. **Termination.** Upon termination or expiration of the Agreement and following Customer's written request, Databricks will delete or assist Customer in deleting any Personal Data within its possession or control within thirty (30) days following such request.

10. CCPA Compliance

10.1. Databricks shall not process, retain, use, or disclose Personal Data for any purpose other than for the purposes set out in the Agreement, DPA and as permitted under the CCPA. Databricks shall not sell or share information as those terms are defined under the CCPA.

11. GENERAL

11.1. The parties agree that this DPA shall replace any existing data processing addendum, attachment, exhibit or standard contractual clauses that the parties may have previously entered into in connection with the Databricks Services.

11.2. This DPA may not be modified except by subsequent written agreement of the parties.

11.3. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

11.4. Databricks' obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions: (a) Customer is solely responsible for communicating any processing instructions on behalf of its Authorized Affiliates; (b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations under this DPA; and (c) if an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Databricks ("**Authorized Affiliate Claim**"), Customer must bring such Authorized Affiliate Claim directly against Databricks on behalf of such Authorized Affiliate, unless Applicable Data Protection Laws require the Authorized Affiliate be a party to such claim, and all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

11.5. In the event of any conflict between this DPA and any data privacy provisions set out in any agreements between the parties relating to the Databricks Services, the parties agree that the terms of this DPA shall prevail, provided that if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses control and take precedence. If there is any conflict between this DPA and a Business Associate Agreement entered into between the parties ("**BAA**"), then the Business Associate Agreement shall prevail to the extent of any conflict solely with respect to any PHI (as defined in such BAA).

11.6. Notwithstanding anything to the contrary in the Agreement or this DPA and to the maximum extent permitted by law, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including all Annexes hereto), the SCCs or any data protection agreements in connection with the Agreement (if any), whether in contract, tort or under any other theory of liability, shall remain subject to the limitation of liability section of the Agreement and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA, including all Annexes hereto. Customer agrees that any regulatory penalties incurred by Databricks that arise in connection with Customer's failure to comply with its obligations under this DPA or any Laws or regulations including Applicable Data Protection Laws shall reduce Databricks' liability under the Agreement as if such penalties were liabilities to Customer under the Agreement.

11.7. This DPA will be governed by and construed in accordance with Federal law. A US Government Customer shall not comply with any provision of this DPA, EU law, or the law of an EU Member State that is inconsistent with US Federal law.

11.8. The obligations placed upon each party under this DPA and the Standard Contractual Clauses shall survive so long as Databricks processes Personal Data on behalf of Customer.

[SIGNATURE PAGE FOLLOWS]

By signing below, each party acknowledges that it has read and understood the terms of this DPA and agrees to be bound by them.

Customer:_____	**Databricks, Inc.**
By:_____	By:_____
Name:_____	Name: Scott Starbird
Title:_____	Title: General Counsel, Public Affairs Strategic and Partnerships
Date:_____	Date:_____
Contact Person:_____	
Contact Title:_____	
Contact Email:_____	

ANNEX A

DESCRIPTION OF THE PROCESSING / TRANSFER

ANNEX 1(A): LIST OF PARTIES	
Data exporter	**Name of the data exporter:** The entity identified as the "Customer" in the Agreement and this DPA. **Contact person's name, position and contact details:** The address and contact details associated with Customer's Databricks account, or as otherwise specified in this DPA or the Agreement. **Activities relevant to the data transferred:** The activities specified in Annex 1(B)below. **Signature and date**: See front end of the DPA.
Data importer	**Role (Controller/Processor):** Controller (for Module 2) or Processor (for Module 3). **Name of the data importer:** Databricks, Inc. **Contact person's name, position and contact details:** Scott Starbird, General Counsel, Public Affairs and Strategic Partnerships, dpa@databricks.com **Activities relevant to the data transferred:** The activities specified in Annex 1.B below. **Signature and date**: See front end of the DPA. **Role (Controller/Processor):** Processor

ANNEX 1(B): DESCRIPTION OF THE PROCESSING / TRANSFER	
Categories of data subjects whose personal data is transferred:	Data subjects include individuals about whom data is provided to Databricks via the Databricks Services (by or at the direction of Customer), which shall include: IF CUSTOMER HAS NOT FILLED OUT THE ABOVE SECTION: Customer shall be deemed to have declared that the categories of data subjects include: (a) individual contacts, prospects, customers, business partners and vendors of Customer (who are natural persons); (b) employees or contact persons of Customer's prospects, customers, business partners and vendors; (c) employees, agents, advisors, freelancers of Customer (who are natural persons); (d) Customer's Authorized Users or (e) other individuals whose personal data is included in Customer Content.
Categories of personal data transferred:	The types of Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

	IF CUSTOMER HAS NOT FILLED OUT THE ABOVE SECTION: Customer shall be deemed to have declared that the types of Personal Data may include but are not limited to the following types of Personal Data: (a) name, address, title, contact details; and/or (b) IP addresses, cookies data, location data; and (c) any other personal data processed in the course of the Services as Customer Content.
Sensitive data transferred (if appropriate)	Subject to any applicable restrictions and/or conditions in the Agreement and this DPA, Customer may include 'special categories of personal data' or similarly sensitive personal data (as described or defined in Applicable Data Protection Laws) in Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health and/or data concerning a natural person's sex life or sexual orientation.
Frequency of the Transfer **Nature, subject matter and duration of the processing:**	Continuous or one-off depending on the services being provided by Databricks. Nature: Databricks provides a cloud-based unified data analytics platform and related services, as further described in the Agreement. Subject Matter: Personal Data. Duration: The duration of the processing will be for the term of the Agreement and any period after the termination or expiry of the Agreement during which Databricks processes Personal Data.
Purpose(s) of the data transfer and further processing:	Databricks shall process Personal Data for the following purposes: (a) as necessary for the performance of the Databricks Services and Databricks' obligations under the Agreement (including the DPA), including processing initiated by Authorized Users in their use and configuration of the Databricks Services; and (b) further documented, reasonable instructions from Customer agreed upon by the parties (the "**Purposes**").
Period for which the personal data will be retained:	Databricks will retain Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Databricks processes Personal Data in accordance with the Agreement.
ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY	
Competent supervisory authority	The data exporter's competent supervisory authority will be determined in accordance with the EU GDPR.

ANNEX B

STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)

1. Subject to Section 8.1 of the DPA, where the transfer of Personal Data to Databricks is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form part of the DPA as follows:

a. In relation to transfers of Personal Data protected by the EU GDPR, the SCCs shall apply as follows:

I. Module Two terms shall apply (where Customer is the controller of Personal Data) and the Module Three terms shall apply (where Customer is the processor of Personal Data);

II. in Clause 7, the optional docking clause shall apply and Authorized Affiliates may accede the SCCs under the same terms and conditions as Customer, subject to mutual agreement of the parties;

III. in Clause 9, option 2 ("**general authorization**") is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in Section 4.3 of the DPA;

IV. in Clause 11, the optional language shall not apply;

V. in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;

VI. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

VII. Annex I shall be deemed completed with the information set out in Annex A to the DPA; and

VIII. Annex II shall be deemed completed with the information set out in the Security Addendum, subject to Section 6.1 (Security Measures) of the DPA.

b. In relation to transfers of Personal Data protected by the UK GDPR, the SCCs as implemented under Section 1(a) above shall apply with the following modifications:

I. the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;

II. Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex A and Annex B to the DPA and the Security Addendum respectively, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and

III. any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

c. In relation to transfers of Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1(a) above will apply with the following modifications:

I. references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

II. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and/or "Swiss law" (as applicable);

III. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland");

IV. the SCCs shall be governed by the laws of Switzerland; and

V. disputes shall be resolved before the competent Swiss courts.

2. Where the Standard Contractual Clauses apply pursuant to Section 8.1 of this DPA, this section sets out the parties' interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a party complies with the interpretations set out below, that party shall be deemed by the other party to have complied with its commitments under the Standard Contractual Clauses:

a. where Customer is itself a processor of Personal Data acting on behalf of a third-party controller and Databricks would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), Databricks may interact solely with Customer and Customer shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;

b. the certification of deletion described in Clause 16(d) of the SCCs shall be provided by Databricks to Customer upon Customer's written request;

c. for the purposes of Clause 15(1)(a) the SCCs, Databricks shall notify Customer and not the relevant data subject(s) in case of government access requests, and Customer shall be solely responsible for notifying the relevant data subjects as necessary; and

d. taking into account the nature of the processing, Customer agrees that it is unlikely that Databricks would become aware of Personal Data processed by Databricks is inaccurate or outdated. To the extent Databricks becomes aware of such inaccurate or outdated data, Databricks will inform the Customer in accordance with Clause 8.4 SCCs.

Advisory Services Schedule

This Schedule sets forth terms related to the Advisory Services and is incorporated as part of the Master Cloud Services Agreement ("**MCSA**"). The MCSA and this Schedule, together with any other Schedules that reference or are otherwise incorporated into the MCSA comprise the Agreement. This Schedule will co-terminate with the MCSA. Other Schedules do not apply to the services ordered under this Schedule unless expressly referenced as being applicable. Capitalized terms used but not defined in this Schedule have the meaning assigned to them in the MCSA.

1. **Additional Definitions.**

    1. **"Advisory Services DPA"** means, unless Customer has entered into the Platform Services DPA , the Data Processing Addendum for non-Platform Services attached hereto and located at databricks.com/legal/non-platform-dpa.
    2. **"Customer Materials"** means the information and materials you provide to Databricks for Databricks to perform the Advisory Services.

2. **Advisory Services.**

    1. **Generally.** Subject to the Order, Databricks will provide Advisory Services to facilitate your use of the Databricks platform. Unless otherwise agreed by the parties, Advisory Services will expire one year after the Start Date indicated on the Order and will be booked on the basis of 8-hour service days.
    2. **Intellectual Property.**

        1. **License**. Upon your payment of all Fees under an applicable Order, Databricks grants you a non-exclusive, perpetual, fully paid-up, royalty-free license to use, copy, modify, or create derivative works based on any Advisory Services work product delivered by Databricks to you under the Order (the **"Deliverables"**). If and to the extent Databricks incorporates any Databricks Materials (as defined below) into the Deliverables, Databricks grants to you a non-exclusive, perpetual, fully paid-up, royalty-free license to use, copy, modify or create derivative works based on such Databricks Materials, solely as incorporated into the Deliverables and solely for your internal business use as reasonably necessary to use the Deliverables for their intended purposes. For the avoidance of doubt, no part of the Platform Services will be deemed to be incorporated into the Deliverables.
        2. **Databricks Materials**. Subject to your rights in your Confidential Information, Databricks will exclusively own all rights, title and interest in and to: (i) the Deliverables; and (ii) any software programs, tools, utilities, processes, inventions, devices, methodologies, specifications, documentation, techniques, training materials, and other materials of

any kind used or developed by Databricks or its personnel in connection with performing the Advisory Services, or any other Databricks Services (collectively **"Databricks Materials"**), including all Intellectual Property Rights in any of the foregoing.

3. **No Maintenance**. Unless otherwise set forth in an Order the Deliverables are not subject to any maintenance, support or updates after the termination of the Order.

3. **Requirements; Limitations.** Databricks will provide the Advisory Services remotely or at a mutually agreed location. While on Customer's premises, Databricks will adhere to reasonable policies provided by Customer in writing in advance. For the avoidance of doubt, no such policies will be deemed to modify the terms of the Agreement.
4. **Use of Workspace during Performance of Advisory Services.** You may be required to use a Workspace in order to receive Advisory Services. Your use of the Workspace constitutes acceptance of the Platform Services terms of the MCSA unless the Workspace is provided as part of a Databricks Powered Service.

3. **Your Obligations; Customer Materials.**

1. **Your Responsibilities.** You:

1. are responsible for taking reasonable steps at all times to maintain the security, protection and backup of all Customer Materials, including within the Platform Services and any Customer Systems;
2. acknowledge that: (i) Databricks does not provide data backup services; and that (ii) Databricks is not responsible for any loss, destruction, alteration, unauthorized disclosure or corruption of Customer Materials not caused by the gross negligence or willful misconduct of Databricks or any third party under the control of Databricks;
3. agree not to provide Databricks with access to more data than is reasonably necessary to permit Databricks to perform the Advisory Services; and
4. acknowledge that successful delivery of the Advisory Services depends on your full and timely cooperation. You agree to make available any reasonably requested personnel and/or information in a timely manner to allow Databricks to perform such services.

2. **Restrictions on Use.** You will not:

1. copy, modify, disassemble, decompile, reverse engineer, or attempt to view or discover the source code of any Deliverables provided to you in object code, in whole or in part, or permit or authorize a third party to do so, except to the extent such activities are expressly permitted by the Agreement or by law notwithstanding this prohibition;

2. use the Databricks Services to develop or offer a service made available to any third party that could reasonably be seen to serve as a substitute for such third party's possible purchase of any Databricks product or service; or
3. transfer or assign any of your rights hereunder except as permitted under Section 11.4 (Assignment) of the MCSA.

3. **Customer Materials.** You represent and warrant to Databricks that Customer Materials will not contain:

1. any data for which you do not have all rights, power and authority necessary for its collection, use and processing as contemplated by the Agreement; or
2. except as otherwise specified in an Order, any (x) bank, credit card or other financial account numbers or login credentials, (y) social security, tax, driver's license or other government-issued identification numbers, or (z) health information identifiable to a particular individual.

4. **Data Protection**. Databricks will maintain appropriate administrative, physical, and technical safeguards according to ISO/IEC 27001:2013 (the **"ISMS Standard"**) for protection of the security and confidentiality of Customer Materials under Databricks' control. Unless specified otherwise in an Order, Databricks engages in the performance of Advisory Services with the expectation that Customer is not engaging Databricks for the purpose of having Databricks act as a data processor for Customer. Nevertheless, except with respect to free Advisory Services, unless you have entered into the Platform Services DPA, the terms of the Advisory Services DPA are hereby incorporated by reference and will apply to the extent Databricks is deemed to act as Customer's data processor during the performance of Advisory Services when the Customer Materials include Personal Data, as defined in the Advisory Services DPA. This Schedule and the Advisory Services DPA do not govern the protection of Customer Content and Databricks does not act as a data processor with respect to any data processed by or within a Databricks Powered Service.

1. **Expenses.** Any Contractor travel required in the performance of services must comply with Public Law 99-234 and FAR Part 31.205-46, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel.
2. **Warranties; Disclaimer.**

1. **Warranties.** Databricks warrants that the Advisory Services will be provided in a professional and workmanlike manner consistent with industry standards. You must notify Databricks of any warranty deficiencies within ninety (90) days from performance of the deficient Advisory Services. Unless set forth in an Order Databricks makes no guarantee as to whether the Advisory Services will be completed within any specific time frame.

2. **Disclaimer**. THE WARRANTIES IN SECTION 6.1 (WARRANTIES) ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, REGARDING THE DATABRICKS' SERVICES PROVIDED HEREUNDER. DATABRICKS SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, CONDITIONS AND OTHER TERMS INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES, CONDITIONS AND OTHER TERMS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO ANY OF THE FOREGOING. NOTWITHSTANDING ANYTHING TO THE CONTRARY HEREIN: (i) SERVICES PROVIDED UNDER ANY FREE TRIAL PERIOD ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND BY DATABRICKS; (ii) WITHOUT LIMITATION, DATABRICKS DOES NOT MAKE ANY WARRANTY OF ACCURACY, COMPLETENESS, TIMELINESS, OR UNINTERRUPTABILITY, OF THE DATABRICKS SERVICES; AND (iii) DATABRICKS IS NOT RESPONSIBLE FOR RESULTS OBTAINED FROM THE USE OF THE DATABRICKS SERVICES OR FOR CONCLUSIONS DRAWN FROM SUCH USE.
3. **Exclusive Remedy**. FOR ANY BREACH OF THE WARRANTY AT SECTION 6.1 (WARRANTIES), YOUR EXCLUSIVE REMEDY AND DATABRICKS' ENTIRE LIABILITY WILL BE THE RE-PERFORMANCE OF THE DEFICIENT SERVICES, OR, IF DATABRICKS CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER, DATABRICKS WILL END THE DEFICIENT SERVICES AND REFUND TO YOU THE PORTION OF ANY PREPAID FEES PAID BY YOU TO DATABRICKS APPLICABLE TO THE PERIOD FOLLOWING THE COMMENCEMENT OF THE DEFICIENCY.

3. **Additional Indemnities.** Reserved.

Public Sector Services Schedule

This Schedule sets forth terms related to use by Public Sector Customers of Databricks Services and is incorporated as part of the Master Cloud Services Agreement (the "**MCSA**"). The MCSA and this Schedule, together with any other Schedules that reference or are otherwise incorporated into the MCSA comprise the Agreement. This Schedule will co-terminate with the MCSA. Capitalized terms used but not defined in this Schedule have the meaning assigned to them in the MCSA.

1. **Contracting Entity and Order of Precedence.** If an Order identifies the Databricks contracting party as Databricks Federal, LLC ("**DBF**"), then any references in the Agreement to Databricks, including those contained in this Schedule, will be deemed to refer to DBF. Orders referencing DBF or any Order between Databricks and a Public Sector Customer will be deemed to incorporate this Schedule. In the event of a conflict between this Schedule and the MCSA or another Schedule thereto, this Schedule will be deemed to control solely for such DBF Order or other Public Sector Order.
2. **Databricks Services.** This Schedule establishes the terms and conditions enabling Databricks to provide Databricks Services to Public Sector Customers. For the purposes of this Schedule, references to "Customer" in an Order, the MCSA or any Schedule thereto will be deemed to refer to Public Sector Customer or Customer Representative, as applicable. This Schedule does not grant you access to the Databricks Services without mutual agreement to an Order and applicable Databricks Services Schedule.
3. **Additional Definitions.**
    1. **"Customer Information"** means Customer Content (if you are purchasing Platform Services) and / or Customer Materials (if you are purchasing Advisory Services).
    2. **"Customer Representative"** means an organization authorized on behalf of a Public Sector Customer to purchase Databricks Services on its behalf, as designated in an applicable Order.
    3. **"Federal Customer"** means any United States federal government branch or agency Customer of Databricks Services subject to this Schedule, including agencies and departments from the Executive Branch, the Congress, or the Military.
    4. **"Public Sector Customer"** means any Federal Customer or other United States state or local government, or entity, authority, agency, or body exercising executive, legislative, judicial, regulatory or administrative functions of any such government, who purchases Databricks Services subject to this Schedule. Public Sector Customer(s) may include public universities and hospitals.
4. **Modification.** Notwithstanding anything contained in the MCSA or any other Schedule, you agree as follows:

1. **U.S. Government License Rights.** If Customer is a Federal Customer, or the Agreement otherwise become subject to the Federal Acquisition Regulation (FAR), Customer acknowledges and agrees that the Platform Services (including PVC Services, as applicable), Support Services (as applicable), and accompanying documentation constitute "commercial computer software" and "commercial computer software documentation", respectively, provided as "Commercial Items" as defined in FAR 2.101. The Platform Services (including PVC Services, as applicable), Support Services (as applicable), and accompanying documentation have been developed solely at private expense, and as set forth in FAR 12.212, any use, modification, reproduction release, performance, display or disclosure thereof shall be solely in accordance with the terms of the MCSA as modified by this Schedule.
2. **Customer Representative Obligations.** Customer Representative will have no rights to the Databricks Services if purchasing Databricks Services on behalf of a Public Sector Customer except to the extent that a Public Sector Customer provides access to Customer Representative as its Authorized User. Customer Representative agrees to bind Public Sector Customer to the terms of the Agreement, including this Schedule. Customer Representative acknowledges that submission of a purchase order or Order will be deemed to be a representation to Databricks that the applicable Public Sector Customer has assented to the terms of the Agreement. Customer Representative will use commercially reasonable efforts to enforce the terms of the Agreement in the event it becomes aware that the Public Sector Customer has breached any terms and conditions of the Agreement where such breach adversely affects Databricks' rights or contractual protections. Customer Representative will notify Databricks promptly upon learning of any such breach.
3. **Acceptance.** Reserved.
4. **Confidentiality.** Any provisions contained in the Agreement that require a Public Sector Customer to keep certain information confidential may be subject to the Freedom of Information Act, 5 U.S.C. §552 or similar applicable state or local state law, and any order by a United States Federal Court or court of appropriate jurisdiction.
5. **Equitable Relief.** Orders entered into directly with Databricks by a Federal Customer subject to this Schedule will only allow equitable relief when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act).
6. **Auto Renewal, Customer Responsibility, and Indemnification.** If you are a Federal Customer subject to the Anti-Deficiency Act or similar limitations on fees or payment absent approved allocation of funding, any auto-renewal of Databricks Services, penalty fees or interest accrual associated with late payment, or Customer indemnification obligations in the Agreement will be deemed inapplicable. Any clause in the Agreement requiring Databricks to defend or indemnify a Public Sector Customer is hereby amended solely to the

extent that (a) the U.S. Department of Justice has the sole right to represent the Federal Customers in any such action in accordance with 28 U.S.C. 516, and (b) representation on behalf of Public Sector Customers may lie solely with the applicable state attorney general's office if you are a state or local government entity.

7. **Governing Law.** This Schedule, the MCSA, and any other applicable Schedules is governed by Federal law. If you are a state or local government entity, the Agreement is governed by the laws of your state, excluding its conflict of laws principles. In the event the Uniform Computer Information Transactions Act (UCITA) or any similar laws or regulations are enacted, to the extent allowed by law, such law or regulation will not apply to the Agreement, and the governing law will remain as if such law or regulation had not been enacted. The Agreement does not affect statutory rights that cannot be waived or changed by contract.
8. **Disputes.** Notwithstanding any other provision in the Agreement, any dispute between Databricks and any Federal Customer arising under or related to the Agreement will be resolved exclusively under the terms and procedures of General Services Administration Acquisition Regulation (GSAR) 552.212-4(w)(1)(iii) Law and Disputes.
9. **Assignment.** Assignment shall be governed by FAR 52.212-4(b) Assignment and GSAR 552.212-4(w)(1)(xi) Non-assignment.
10. **Taxes.** Taxes shall be governed by FAR 52.212-4(k) Taxes and GSAR 552.212-4(w)(1)(x) Taxes and surcharges.