CONFLUENT

CONFLUENT PLATFORM AGREEMENT FOR U.S. PUBLIC SECTOR

This Confluent Platform Agreement for U.S. Public Sector ("Agreement") between Confluent Federal, LLC ("Confluent") and the purchaser or user ("Customer") of Confluent Software, Support Services, and/or any professional and education services ("Confluent Offerings") governs the use of such Confluent Offerings where Customer is a part of a federal, state, or local government within the United States. The effective date of this Agreement ("Effective Date") is the effective date of the relevant Order or agreement providing for the use of the Confluent Offerings. By entering into an Order, Customer is agreeing to and accepting the terms of this Agreement. You represent and agree that you have the legal authority to bind the government entity or agency on whose behalf you are accepting this Agreement, and the rights granted under this Agreement are expressly conditioned upon such authority. If Customer does not accept the terms of this Agreement, then Customer cannot use the Confluent Offerings.

1. LICENSE AND SUPPORT

1.1 License to Confluent Platform. Orders entered into by Customer will specify the Confluent Software purchased by Customer, associated Support Services, plus any related professional services purchased thereunder. Confluent Software is licensed and not sold. Subject to the terms of this Agreement and the applicable Order, Confluent grants to Customer a limited, non-exclusive, non-sublicensable, non-transferable license during the subscription term specified in the applicable Order to install and use Confluent Software solely for Customer's internal business operations. Confluent reserves all rights not expressly granted in this section.

1.2 Affiliates and Service Providers. Customer may permit its Affiliates to use Support Services and Confluent Software purchased by Customer provided that: (i) Customer shall remain responsible for each such Affiliate's compliance with the terms of this Agreement, and (ii) any such use together with Customer's use must be, in the aggregate, within the use limitations set forth in the applicable Order. Customer may permit its third-party service providers to install and use the Confluent Software to provide outsourced services to Customer, and Customer will be solely responsible for such service provider's compliance with this Agreement.

1.3 Restrictions on Use. Customer shall not, and shall not permit or encourage any third party to: (a) use the Confluent Software for third-party training, software-as-a-service, time-sharing or service bureau use; (b) disassemble, decompile or reverse engineer any portions of the Confluent Software that are not provided in source code format; or (c) attempt to gain access to the Confluent Software source code or the underlying ideas, algorithms, structure or organization of the object code. The foregoing restriction is inapplicable to the extent prohibited by applicable law.

1.4 Copies. Customer may make copies of the Confluent Software as reasonably necessary to exercise the license granted in Section 1.1, and a reasonable number of back-up or archival copies, provided that each such copy shall include Confluent's copyright and any other proprietary notices that appear on the original copies of the Confluent Software.

1.5 Certification; Confluent Audit Rights. Upon Confluent's written request, Customer shall certify in writing that it is in full compliance with this Agreement, including all use limitations set forth in each applicable Order. Such certification shall be signed by an officer of Customer. In addition, Confluent reserves the right, upon prior notice to Customer and during normal business hours, to audit Customer's usage of the Confluent Software and Customer's compliance with the terms of this Agreement, provided Confluent personnel

adhere to reasonable security and access requirements under established government policies. If Customer certifies to non-compliance, or Confluent determines as a result of such audit that Customer has exceeded its use limitations, Confluent shall notify Customer of its findings, and Customer will execute new Order(s) to encompass the higher use amount. Customer shall be required to pay amounts due, along with interest in an amount governed by the Prompt Payment Act (31 USC 3901 et seq) and Treasury regulations at 5 CFR 1315. Customer will not be responsible for interest or reimbursing Confluent for audit costs under this Section 1.5 where such payments would violate the Anti-Deficiency Act (31 U.S.C. 1341).

1.6 Delivery of Materials. The Confluent Software, and any versions, updates or maintenance releases of any component thereof, will be delivered only through electronic transfer. The parties shall reasonably cooperate to effectuate such delivery via FTP or other reasonable means.

1.7 Support Services. Confluent will provide the Support Services purchased by Customer as specified in the applicable Order.

1.8 Third Party Software. Confluent also makes available certain Third Party Software. The Third Party Software shall be subject to the applicable third party license(s) and not this Agreement. To the extent the terms of third party licenses applicable to Third Party Software prohibit any of the restrictions in this Agreement, such restrictions will not apply to such Third Party Software. To the extent the terms of third party licenses applicable to Third Party Software require Confluent to make an offer to provide source code or related information in connection with the Third Party Software, such offer is made.

2. USAGE DATA; TELEMETRY METRICS. Confluent may collect data related to Customer's use of Confluent Platform ("Usage Data"). Such Usage Data may be used by Confluent for the provision, improvement, and support of Confluent Platform, including the creation of analytics data. Confluent will not publicly disclose Usage Data, unless such data is aggregated and anonymized or to the extent required by law. Customer acknowledges that certain features of the Confluent Platform may be configured to collect and report on system performance ("Telemetry Metrics") to Confluent. Customer may enable or disable transmission of Telemetry Metrics to Confluent at any time.

3. ORDERS, FEES AND RELATED

3.1 Orders Generally. All Orders are subject to the terms of this Agreement and are not binding until accepted by Confluent.

3.2 Indirect Orders. Sections 3.3 to 3.5 apply only to Orders placed directly with Confluent. If Customer purchases through a reseller, Customer will pay such reseller for such purchase and different payment terms may apply.

3.3 Fees and Payment. Customer shall pay Confluent or its authorized reseller as applicable the fees in the amount set forth in the applicable Order in accordance with the Order terms.

3.4 Taxes. Confluent or its authorized reseller as applicable shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

3.5 Payment Terms. Except as otherwise set forth in the applicable Order, all amounts payable to Confluent under this Agreement will be due within thirty (30) days from the date of an invoice receipt..

4. OWNERSHIP

4.1 Confluent Materials. Confluent or its licensors retain all rights, title and interest, in and to all intellectual property rights in the Confluent Software, including all related and underlying technology and Documentation; and any derivative works, changes, corrections, bug fixes, enhancements, updates and other modifications, or improvements of any of the foregoing ("Modifications"), (collectively, "Confluent Materials"). Except for the express limited rights set forth under this Agreement, no right, title or interest in any Confluent Materials is granted to Customer. Customer acknowledges that the licenses granted in Section 1.1 do not include the right to prepare any Modifications of the Confluent Materials. Confluent reserves all rights not expressly granted in this Agreement. No rights are granted by implication or estoppel.

4.2 Feedback. Customer has no obligation to provide Confluent any suggestions, enhancement requests, recommendations, or other feedback regarding Confluent's products and services ("Feedback"). However, Confluent may use and include any Feedback that Customer provides regarding Confluent's products and services without restriction or payment.

5. CONFIDENTIALITY

5.1 Confidentiality Obligations. Each party shall retain in confidence the non-public information and know-how disclosed or made available by the other party pursuant to this Agreement which is (a) designated in writing as proprietary and/or confidential, if disclosed in writing, (b) if disclosed orally, is designated in writing (which may be via email) as confidential within thirty (30) days of the oral disclosure, or (c) should reasonably be understood to be confidential by the recipient ("Confidential Information"). Notwithstanding any failure to so designate it, Confidential Information of Confluent includes the Confluent Materials, the terms of this Agreement, and all Orders hereunder . Each party shall (x) maintain the confidentiality of the other party's Confidential Information using the same degree of care that it uses to protect the confidentiality of its own similar Confidential Information and at least a reasonable degree of care; (y) refrain from using the other party's Confidential Information except for the purpose of performing its obligations under this Agreement; and (z) not disclose Confidential Information to any party except to its and its Affiliate's employees, subcontractors and agents as is reasonably required in connection with this Agreement and who are subject to confidentiality obligations at least as protective as those set forth in this section. The foregoing obligations will not apply to Confidential Information of the other party which (i) is or becomes publicly known without breach of this Agreement; (ii) is discovered or created by the receiving party without use of, or reference to, the Confidential Information of the disclosing party, as shown in records of the receiving party; or (iii) is otherwise known to the receiving party without confidentiality restrictions and through no wrongful conduct of the receiving party. Receiving party may disclose Confidential Information to the extent required by law or court order (including where Customer is the receiving party and is subject to the U.S. Freedom of Information Act (5 U.S.C. 552) or similar public or open records law) if the receiving party provides prompt notice and reasonable assistance to the disclosing party to enable the disclosing party to seek a protective order or otherwise prevent or restrict such disclosure; and provided that any information so disclosed retains its confidentiality protections for all other purposes.

5.2 Reserved.

6. WARRANTY

6.1 Mutual Warranties. Each party represents and warrants to the other that it has full corporate right and authority to enter into and perform this Agreement.

6.2 Confluent Warranties. Confluent represents and warrants that (i) it shall perform Support Services in a professional manner, employing a standard of care, skill and diligence consistent with industry standards, and (ii) for a period of thirty (30) days after the first delivery of the Confluent Software by Confluent to Customer, the Confluent Software in the form delivered by Confluent to Customer, will perform in all material respects in accordance with the Documentation. This limited warranty shall not apply if the Confluent Software has been altered or modified; or used, adjusted, installed or operated other than in accordance with this Agreement or the instructions furnished by Confluent. Confluent's sole liability and Customer's exclusive remedies for a breach of the foregoing warranties will be for Confluent to correct any failure of the Confluent Software to conform to the Documentation or to re-perform the Support Services in accordance with the requirements stated in the Support Services policy, as applicable. The foregoing warranties will not apply unless Customer notifies Confluent of the nonconformity in writing within thirty (30) days of the date on which Customer first became aware of such nonconformity.

6.3 Warranty Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS AGREEMENT, CONFLUENT MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE CONFLUENT SOFTWARE OR ANY OTHER MATERIALS OR SUPPORT SERVICES PROVIDED HEREUNDER. CONFLUENT SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. EXCEPT AS EXPRESSLY PROVIDED HEREIN, THE CONFLUENT SOFTWARE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS.

7. INFRINGEMENT INDEMNIFICATION. Confluent will defend Customer from and against any claim, demand or lawsuit brought against Customer by a third party alleging that the Confluent Software, as provided to Customer by Confluent and used pursuant to this Agreement, infringes such third party's intellectual property rights, and Confluent will pay such damages or costs as are finally awarded against Customer attributable to such action, provided that Customer gives Confluent: (a) notification in writing of any such action within sixty (60) days of Customer's receipt thereof; (b) sole control of the defense or settlement of such action (provided any settlement releases Customer from all liability), except as prohibited by 28 U.S.C. 516, in which case Customer will consult with Confluent regularly during such action and Confluent will retain the right to intervene in the proceedings at its own expense, through counsel of its choice; and (c) all reasonable information and assistance, at Confluent's expense. If the Confluent Software becomes, or in the opinion of Confluent is likely to become, the subject of such an infringement claim, Confluent shall, at its option, either: (i) procure for Customer the right to use the allegedly infringing element of the Confluent Software, at no charge to Customer; (ii) replace or modify, in whole or in part, the Confluent Software to make it non-infringing; or (iii) if neither (i) or (ii) are commercially available, terminate the applicable Order, accept return of the Confluent Software, and refund a pro rata portion of the fees paid by Customer for the then-current Order term. Confluent assumes no liability hereunder for any claim of infringement if such claim is based on: (a) use of software other than a current unaltered release of the Confluent Software, as provided by Confluent to Customer; (b) the combination, operation or use of the Confluent Software, with non-Confluent programs or hardware, if the claim would not have arisen but for such combination, operation or use; (c) any alteration or modification of the Confluent Software by a party other than Confluent, (d) Apache Kafka, Apache Flink, or any other Third Party Software, or (e) use of the Confluent Software, or any component thereof, other than in accordance with and pursuant to this Agreement. THIS SECTION SETS FORTH CONFLUENT'S ENTIRE LIABILITY AND OBLIGATION AND CUSTOMER'S SOLE REMEDY FOR ANY CLAIM OF INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS. If Customer is a part of the U.S. Government and written approval of the Attorney General is required for Customer to accept the above procedures, Confluent will defend and indemnify Customer as described above only upon such approval.

8. LIMITATION OF LIABILITY

8.1 NOTHING IN THIS AGREEMENT LIMITS EITHER PARTY'S (I) LIABILITY FOR PERSONAL INJURY, DEATH OR WILLFUL MISCONDUCT, (II) LIABILITY THAT CANNOT BE LIMITED BY APPLICABLE LAW, (III) LIABILITY FOR BREACH OF SECTIONS 1.1 (ORDER AND LICENSE), 1.3 (RESTRICTIONS ON USE) OR 5 (CONFIDENTIALITY), (IV) OBLIGATIONS UNDER SECTION 7 (INFRINGEMENT INDEMNIFICATION), OR (V) CUSTOMER'S PAYMENT OBLIGATIONS UNDER THIS AGREEMENT.

8.2 EXCEPT AS SET FORTH IN SECTION 8.1, IN NO EVENT SHALL EITHER PARTY'S OR ITS AFFILIATES' LIABILITY ARISING UNDER THIS AGREEMENT EXCEED THE AMOUNT PAID OR PAYABLE BY CUSTOMER DURING THE TWELVE (12) MONTHS IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

8.3 NOTWITHSTANDING ANYTHING TO THE CONTRARY HEREIN, NEITHER PARTY NOR ITS AFFILIATES SHALL BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, INDIRECT, PUNITIVE OR EXEMPLARY DAMAGES, OR FOR LOST PROFITS, BUSINESS, CONTRACTS, REVENUE, GOODWILL, PRODUCTION, ANTICIPATED SAVINGS, OR LOSS OF DATA, OR FOR ANY CLAIM OR DEMAND BY ANY OTHER PARTY, HOWEVER CAUSED, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

9. TERM AND TERMINATION

9.1 Term. This Agreement commences on the Effective Date and will remain in effect until terminated as specified below.

9.2 Termination. If Customer is not a part of the U.S. Government, In accordance with GSA Schedule Contract Clause 552.238-114 Use of Federal Supply Schedule Contracts by Non-Federal Entities (May 2019), either party may terminate this Agreement and any Order upon breach by the other party of any material obligation under this Agreement which has not been cured within thirty (30) days after providing written notice of such breach to the other party. If Customer is a part of the U.S. Government, Confluent shall not have the foregoing termination right unless such remedy is granted after conclusion of applicable dispute resolution processes under applicable law (e.g., the Tucker Act or Contract Disputes Act) or if such remedy is otherwise available under U.S. Federal law. If Customer is not a part of the U.S. Government, Confluent may also terminate this Agreement upon written notice if Customer: (a) terminates or suspends its business; (b) becomes subject to any bankruptcy or insolvency proceeding under Federal or state statute; (c) becomes insolvent or subject to direct control by a trustee, receiver or similar authority; or (d) has wound up or liquidated, voluntarily or otherwise.

9.3 Effect of Termination. Termination or expiry of an Order will not automatically result in termination of this Agreement. The provisions of this Agreement that by their nature extend beyond the termination of this Agreement including without limitation "Orders, Fees and Related", "Ownership", "Confidentiality", "Infringement Indemnification", "Limitation of Liability" and "Term and Termination" will survive termination.

10. GENERAL

10.1 Assignment. Assignment. Neither party may assign or otherwise transfer this Agreement or any rights or obligations hereunder, in whole or in part, whether by operation of law or otherwise, to any third party without the other party's prior written consent, except to an Affiliate or to any successor to its business or assets to which this Agreement relates, whether by merger, sale of assets, sale of stock, reorganization or otherwise. Any purported transfer, assignment or delegation without such prior written consent will be void. Confluent may not perform any assignment under this Agreement which violates the Anti-Assignment Act, 41 U.S.C. 6305. Subject to this section, this Agreement shall be binding upon and inure to the benefit of the parties, and their respective successors and permitted assigns.

10.2 Delays. In the event that either party is unable to perform any of its obligations under this Agreement due to any Act of God, fire, casualty, flood, earthquake, war, strike, lockout, epidemic, destruction of production facilities, riot, insurrection, material unavailability, acts or intervention of governmental authority, or any other cause beyond the reasonable control of the party invoking this section, and if such party used its commercially reasonable efforts to mitigate its effects, such party shall give prompt written notice to the other party, and the time for the performance shall be extended for the period of delay or inability to perform due to such occurrences.

10.3 Governing Law. This Agreement is governed by the Federal laws of the United States (or, if Customer is a part of a state or local government, the laws of that state). The parties disclaim and exclude the application of the United Nations Convention on Contracts for the International Sale of Goods.

10.4 Export Compliance. Confluent Materials are subject to export control laws and regulations. Customer may not access or use the Confluent Materials or any underlying information or technology except in full compliance with all applicable United States export control laws. Neither the Confluent Technology nor any underlying information or technology may be accessed or used (a) by any individual or entity in any country to which the United States has embargoed goods; or (b) by anyone on the U.S. Treasury Department's list of specially designated nationals or the U.S. Commerce Department's list of prohibited countries or debarred or denied persons or entities.

10.5 U.S. Government Rights. The Confluent Software and Confluent Materials are developed at private expense, and are licensed to the U.S. Government as "commercial items;" "commercial computer software," "commercial computer documentation," and "technical data;" as those terms are defined in 48 C.F.R. Ch 1 ("FAR") and 48 C.F.R. Ch. 2 ("DFARS"). Customer agrees that Confluent Software, Support Services, and professional and educational services are commercial products and commercial services under FAR 2.101. Any use, modification or disclosure of the Confluent Software or Confluent Materials is subject solely to the terms of this Agreement and any other restrictions that generally apply to the Confluent Software or Confluent Materials.

10.6 Other. This Agreement, together with and inclusive of any referenced exhibits, addenda and any incorporated terms, represents the entire agreement between the parties, and supersedes all prior agreements and understandings, written or oral, with respect to its subject matter, and is not intended to confer upon any third-party any rights or remedies. Customer acknowledges that it has not relied on any representations other than those contained in this Agreement. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, shall be effective unless in writing and signed by both parties. In the event of a conflict between the terms of this Agreement and an Order, the terms of

the Order shall prevail. The terms of this Agreement will supersede any additional or conflicting term in any other purchasing-related document issued by Customer and relating to an Order. The waiver of one breach or default or any delay in exercising any rights will not constitute a waiver of any subsequent breach or default. If any provision of this Agreement is held invalid or unenforceable under applicable law by a court of competent jurisdiction, it will be replaced with the valid provision that most closely reflects the intent of the parties and the remaining provisions of this Agreement will remain in full force and effect. Confluent may use and display Customer's name and logo on the Confluent website and in Confluent marketing and sales materials for Confluent Platform. Nothing in this Agreement will be construed as creating an agency, partnership, or joint venture relationship between the parties. Neither party shall have any right or authority to assume or create any obligations or to make any representations or warranties on behalf of the other party, whether express or implied, or to bind the other party in any respect. Confluent will provide any required notice to Customer under this Agreement by sending the notice by email to the email address that Customer provides to Confluent for its account. To provide notice to Confluent under this Agreement, Customer must send the notice, expressly referencing this Agreement and section with respect to which Customer is providing notice, by email to legal@confluent.io.

11. DEFINITIONS

11.1 "Affiliate" means any entity that controls, is controlled by, or is under common control with a party, where "control" means direct or indirect ownership of more than 50% of the voting interests of the entity.

11.2 "Confluent Platform" is Confluent Software together with Apache Kafka and/or Apache Flink.

11.3 "Confluent Software" means Confluent's proprietary software that is licensed and used pursuant to the applicable Order.

11.4 "Documentation" means the published documentation describing the functionality of the Confluent Software located at https://docs.confluent.io/current/.

11.5 "Order" means an ordering document for Confluent Platform, Support Services, and/or any professional and education services, entered into by Customer with either Confluent or a Confluent-authorized reseller, in accordance with the applicable Confluent Platform definitions and rules posted at confluent.io/contracts.

11.6 "Support Services" means the applicable support and maintenance service that Customer purchases, as may be more fully described in the applicable Order.

11.7 "Third Party Software" means certain third party software that is made available by Confluent as identified in the applicable help, notices, about or source file.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives.

CONFLUENT FEDERAL, LLC	**CUSTOMER: _____**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

Confluent Platform Subscription Definitions and Rules

Effective Date: October 27, 2025

These definitions and rules supplement and are incorporated by reference into your applicable Order with Confluent. All capitalized terms will have the meanings assigned to them in the Order or the Agreement.

Confluent may update these definitions and rules from time to time. Each update will bear an Effective Date, and will apply only to Orders that are entered into after such Effective Date. Any material changes to these definitions and rules will not apply unless and until such changed terms are accepted by Customer. Prior versions (available in the archive on confluent.io/contracts) remain applicable to Orders entered into during the effective period of such versions.

Confluent Platform

The "Confluent Platform" is Confluent Software together with Apache Kafka® and Apache Flink®. The Confluent Software licensed under an Order consists of:

Commercial features	
Kafka Connect Workers	Commercial Connectors *
	Premium Connectors *
Health+*	
Control Center	
Operator (k8s)	
Replicator	
MQTT Proxy	
Secret Protection	
Client-Side Field Level Encryption *	
Confluent Platform for Apache Flink *	
Confluent Server	Role-Based Access Control
	Structured Audit Logs
	Schema Validation
	Multi-Region Clusters**
	Tiered Storage**
	Self-Balancing Clusters
	Cluster Linking
	Auto Data Balancer
Community features	
Kafka Connect Workers	Community-licensed Connectors
REST Proxy	
ksqlDB	
Schema Registry	

* If purchased, as specified in an Order

** Customer is prohibited from using these features with Confluent Platform Edge deployments.

Confluent also makes the community feature software available under the Confluent Community License, and Customer's rights under such license with respect to such software shall not be limited by the terms of the Agreement.

Confluent Private Cloud

Confluent Private Cloud ("CPC") means the licensed software package that includes (a) Confluent Platform, (b) the Confluent Private Cloud Gateway, and (c) other additional functionality Confluent includes with CPC, including Intelligent Replication and CSFLE. Confluent Private Cloud Gateway Nodes are excluded from the CPC Node count used to calculate CPC fees.

A CPC Node is limited to a software instance of running on a physical or virtual computing machine that does not exceed any of the following elements:

- 56 processing cores or virtual cores
- 24 hard drives
- 50 TB total hard drive or flash/SSD capacity
- 256 GB of RAM

Confluent Private Cloud Gateway Node means the stateless, Kafka-protocol-aware proxy that provides intelligent routing and policy enforcement between Kafka clients and Confluent-managed or self-managed clusters.

Subscription Fee Units of Measure

The subscription fees are based on the specified units of measure, as defined below. Customer may not use the Confluent Platform subscription (including Support Services) in a manner that exceeds the quantity it has purchased.

"Node" means each software instance of a Confluent Platform component (identified below) running on a physical or virtual computing machine.

"Confluent Platform component" means any of the following:

- Confluent Server
- Kafka Broker
- Zookeepers / Quorum Controllers**
- Kafka Connect Worker
- Replicator (Kafka Connect Worker)
- Mirror Maker
- Operator
- Control Center*
- Schema Registry
- ksqlDB (formerly KSQL)
- REST Proxy
- MQTT Proxy

*One Node for Control Center for version 2.0.0 and later is equal to the deployment of one instance of Control Center, one instance of Prometheus, and one instance of Alertmanager.

**The Confluent Platform KRaft SKU does not include this as a component.

For the avoidance of doubt, a Node does not include an application that uses only the client API (i.e., Kafka Producer/Consumer).

Flink Node

Each Flink Node may not exceed 8 CPU Cores per Flink Node. A Flink Node must be purchased separately from and is not interchangeable with a Node for a Confluent Platform component without an Order.

Definitions

"CPU" means an actual bare metal processing unit that has at least one CPU Core. Multi-core or hyperthreading processors are counted as one CPU.

"CPU Core" means the central billing unit of the Flink Node, enabling Customer to schedule applications (an abstraction over Flink jobs) up to the number of CPU Cores permitted under the Order. A CPU Core refers to "cpu units" in Kubernetes. One CPU is equivalent to 1 AWS vCPU, 1 GCP core, 1 Azure vCore (or similar concepts for other cloud providers) or 1 hyperthread on a bare-metal processor with hyperthreading enabled.

"Flink Node" means a group of up to 8 CPU cores allocated to software instances of Confluent Platform for Apache Flink running on a physical or virtual computing machine.

As specified in the Order, a Node, Flink Node, Connector Pack, or Premium Connector is classified as one of the following:

- "Production", which means use for any purpose other than the purposes specified below for Pre-Production, Development, and Disaster Recovery. A Production instance also includes instances that are running in Hot Standby Mode, and excludes instances that are installed but not running. Hot Standby Mode describes an active-active setup where instances are continuously mirroring the production environment.
- "Pre-Production", which means use solely for QA, staging, end-user testing or other non-development pre-production purposes.
- "Development", which means use solely by developers testing code, or use solely in a sandbox environment that is not accessed or in any way used by users of the production system.
- "Disaster Recovery" means use solely in any other standby mode besides Hot Standby Mode, e.g., active-passive setups.

Add-On Products

Connector Packs
A "Connector Pack" provides a license and Support Services for up to five (5) commercial connectors per Connector Pack. Confluent's commercial connectors are identified at https://www.confluent.io/product/connectors/#commercial.

Premium Connectors
Customer's purchase of a premium connector includes a license and Support Services for the premium connector designated in the Order.

Health+
Customer acknowledges that certain features of the Confluent Platform may be configured to collect and report telemetry data to Confluent as more particularly described at https://www.confluent.io/moreinformation/. Customer may choose to enable or disable transmission of this data to Confluent at any time; however, the disablement of telemetry data may prevent the provisioning of Health+.

Unified Stream Manager

Fees and Invoicing: Customer agrees to pay Confluent or its authorized reseller as applicable all fees specified in an Order, including all fees incurred for its usage of the Unified Stream Manager ("USM Service").

Billing: The USM Service bills are based on Customer's consumption of resources within Customer's Cloud Organization ID. All billing computations are conducted in Coordinated Universal Time (UTC).

Total Commitment or Total Available Balance: The amount of the USM Service usage fees the Customer may consume prior to being billed overages during the applicable Order Term.

Net Payable Amount: The amount the Customer is committed to pay under an applicable Order, subject to any schedule defined therein. If not stated, it shall be equivalent to the Total Commitment.

New Components and Continued Usage: If Confluent adds new features or components to the USM Service during an applicable Order Term ("New Components") for which Confluent charges separate fees, Confluent will publish supplemented pricing to Customer's Rate Card on or before the date of general availability, and Customer will be charged for usage of such New Components in accordance with such pricing. Any Discount will not be applied to charges for the New Components during the applicable Order Term. If such New Components are initially made available as "Preview" or "Early Access," the pricing may change when the New Components are made generally available.

Support Services: Customer's Support Services plan for the USM Service must correspond to the comparable plan for the applicable Confluent Platform environment that the USM Service is connected to. For example, if the USM Service is connected to a Confluent Platform environment where the Confluent Platform Support Services plan is Platinum then the Support Services plan for the USM Service must be Premier.

Usage Data and Telemetry Metrics: Usage Data and Telemetry Metrics include data related to Customer's use of the USM Service.

ksqlDB

Nodes designated in the Order as ksqlDB Add-on Nodes are specific to instances of ksqlDB, and cannot be allocated to any other instances of Confluent Platform components without an Order.

Client-Side Field Level Encryption ("CSFLE")

Fees for an add-on purchase of CSFLE are based on the number of Nodes within a given cluster that CSFLE is deployed on, which includes all of the Nodes and Flink Nodes within the cluster.

Kafka Streams

Fees for an add-on purchase of Support Services for Kafka Streams are based on Customer's total Nodes under subscription, including any active subscriptions under other orders, but excluding any ksqlDB add-on Nodes. Notwithstanding anything to the contrary in the Support Services policy or elsewhere, Customer is prohibited from using Kafka Streams with Confluent Platform unless it has paid for Support Services for Kafka Streams. If Customer utilizes Kafka Streams without purchasing Support Services for Kafka Streams, then Customer must pay Confluent its then-current list rate for Support Services for Kafka Streams. Support Services

for Kafka Streams applies to an unlimited number of Kafka Streams applications connected to the supported Confluent Platform cluster.

Support Services

Confluent shall provide the Support Services as set forth in the Order and detailed further in the Support Services Policy attached hereto and available at https://www.confluent.io/support-services-policy/. For Confluent Platform Edge, Confluent will provide Support Services for only five named individuals in the Support Portal, except as otherwise approved by Confluent in writing.

If Customer is using Support Services on any Confluent Platform component in a cluster, then (i) all Confluent Platform components in such cluster will be counted as Nodes and must be under subscription, and (ii) Customer must pay all applicable fees required for Support Services for such Confluent Platform components and for add-on products connected to the cluster, including Support Services for Kafka Streams.

CONFLUENT

Support Services Policy
Confluent Platform

Updated June 2, 2025

1. Definitions

1.1 "Business Day" means Monday through Friday in Customer's local time zone.

1.2 "Business Hours" means 9:00 a.m. to 5:00 p.m. on Business Days.

1.3 "Confluent Platform" means Confluent's distribution of Apache Kafka® and Apache Flink® together with Confluent Software.

1.4 "Documentation" means the user and installation documentation for the Supported Software published by Confluent and accessible at https://docs.confluent.io/current/.

1.5 "Issue" means a failure of the Supported Software to conform to the specifications set forth in the Documentation, resulting in the inability to use, or material restriction in the use of, such Supported Software.

1.6 "Maintenance Release" means a revision of the Supported Software made generally available by Confluent to its end user customers to correct Issues in the Supported Software or to maintain the operation of the Supported Software in accordance with the documentation. Maintenance Releases are denoted by a change to the third decimal place in the version number; e.g., 2.1.1, 2.1.2, 2.1.3, etc.

1.7 "Support Request" means a support request or Issue submitted by Customer as described in this Support Services Policy.

1.8 "Support Services" means the maintenance and support services purchased by Customer and described in this Support Services Policy.

1.9 "Supported Software" means the supported versions of Confluent Platform components, as set forth in the Supported Versions and Interoperability document at https://docs.confluent.io/current/installation/versions-interoperability.html.

1.10 "Update" means a software modification or addition that, when made or added to the Supported Software, corrects the Issue.

1.11 "Workaround" means a procedure or routine that, when observed in the regular operation of the Supported Software, eliminates the practical adverse effect of the Issue on Customer.

2. Support Services

2.1 **Applicability.** This Support Services Policy applies to all levels of Support Services for Confluent Platform subscriptions, except to the extent that variations are specifically described herein or in the applicable Order.

2.2 **Customer Support Channels.** Confluent shall provide the Support Services through its online customer support portal ("Support Portal"). Following submission of a Support Request, Confluent will communicate with Customer using email, the Support Portal, or video conferencing. During the submission process, Customer may assign a priority level to an Issue, however, Confluent may

re-assign the priority level in its sole discretion, based on the priority level definitions below and following discussion with Customer regarding the reason for the re-assignment. Any necessary telephone support discussions will be scheduled in advance at a time mutually agreed by the parties and for durations and at a frequency that is commercially reasonable for Confluent. Support Services will be provided in English.

For Platinum-level Support Service, Confluent also will provide a direct phone line for P1 Support Requests in addition to standard communication channels.

2.3 **Hours of Operation**. Customer may submit Support Requests twenty-four (24) hours a day, seven (7) days per week.

2.4 **Support Request Prioritization & Confluent Actions.** Support Requests will be categorized by priority level in accordance with the following definitions, and Confluent will take the following corresponding actions:

Support Request Priority Definitions & Confluent Actions		
Priority Level	**Definition**	**Confluent Actions**
P1	Priority One means that, due to an Issue, (i) the production system is severely impacted or completely shut down, or (ii) the production system operations or mission-critical applications are down.	Confluent will: (i) assign specialists to work continuously to correct the Issue; (ii) provide ongoing communication on the status of an Update or Issue resolution; and (iii) simultaneously begin work to provide a temporary Workaround or fix.
P2	Priority Two means that, due to an Issue, (i) the production system is functioning with limited capabilities, or (ii) the production system is unstable with periodic interruptions. An Issue relating to a non-production application may be classified as P2 provided that the Issue is related to an application in the final stages of development and is either blocking all other development efforts and/or putting the release milestone at risk, and missing such milestone would have a significant impact on Customer's business.	Confluent will: (i) assign specialists to correct the Issue; (ii) provide regular communication on the status of an Update or Issue resolution; and (iii) simultaneously begin work to provide a temporary Workaround or fix.
P3	Priority Three means (i) there are Issues with workaround solutions in	Confluent will assign specialists to be available during local Business Hours

	fully operational production systems, (ii) there are Issues in non-critical functions, (iii) there is a time sensitive Issue affecting performance or deliverables, or (iv) a major subsystem under development cannot proceed due to an Issue.	until the Issue is resolved or a Workaround is in place. For issues in Third Party Software, Confluent will use reasonable efforts to liaise with the applicable project steward.
P4	Priority Four means (i) there is a need to clarify procedures or information in documentation, (ii) there is a request for a product enhancement or new feature, (iii) cosmetic or non-functional Issues; or (iv) issues in the documentation.	Confluent will triage the request, provide clarification where possible, and may include a resolution in a future Maintenance Release.

2.5 **Responses.** A "Response" is an initial reply to a Support Request. "The Target First Response Times" shall be measured by the elapsed time between Confluent's receipt of a Support Request and the time Confluent begins to address it by responding and initiating communication with Customer about the Support Request. The actual time required to fully resolve an Issue or request, if full resolution occurs, may be longer than the Target First Response Time. Customer understands and agrees that full resolution of an Issue is not guaranteed and may not occur.

Target First Response Times		
Priority Level	**Support Level**	
	Gold	**Platinum**
P1	Within 60 minutes	Within 30 minutes
P2	Within 4 hours	Within 2 hours
P3	Within 8 Business Hours	Within 8 Business Hours
P4	Within 2 Business Days	Within 2 Business Days

2.6 **Updates and Maintenance Releases.** Confluent will use commercially reasonable efforts to provide an Update or Workaround designed to solve or bypass a reported Issue, in accordance with the table in sections 2.3 and 2.4 above. Customer will use commercially reasonable efforts to install and implement Maintenance Releases for the installed version of the Confluent Platform as such Maintenance Releases become available. An Update or Workaround may be provided in the form of a temporary fix, procedure or routine, to be used until a Maintenance Release containing an applicable Update is available. Confluent will make Maintenance Releases available to Customer if, as and when Confluent makes any such Maintenance Release generally available to its customers.

2.7 **Customer Responsibilities.** Confluent's provision of Support Services depends upon Customer fulfilling the following responsibilities with respect to each Issue:

(a) Customer making reasonable efforts to resolve the Issue before reporting the Issue to Confluent, including having the Issue reviewed by the representative of Customer that submits the Support Request;
(b) Customer providing Confluent with sufficient information, including a description of the issue, changes made preceding its occurrence and any reproducible test cases requested by Confluent;
(c) Customer making commercially reasonable efforts to install any applicable Maintenance Releases for the installed version of the Confluent Platform as such Maintenance Releases become available;
(d) Customer procuring, installing and properly maintaining all equipment, network connections, communication interfaces and other hardware necessary to operate the Supported Software; and
(e) (For P1 and P2 Issues only) Customer designating personnel resources to provide necessary diagnostic information and engage with Confluent until an Update or Workaround is made available.

2.8 **Escalation**. If Customer does not receive Confluent's Response within the applicable Target First Response Time, Customer may escalate the Support Request to Confluent Support Team Management. An escalation ticket can be opened by setting the Support Request priority to "Manager Escalation" in the support portal.

3. Exclusions. Notwithstanding anything to the contrary in this Support Services Policy or the Agreement, Confluent is not obligated to continue work on a Support Request when Confluent determines that:

(a) the Supported Software has been changed or modified (except if by Confluent or under the direct supervision of Confluent);
(b) the reported issue has been caused by a hardware malfunction, the configuration of the operating environment or data center, network latency or causes in Customer's environment beyond the reasonable control of Confluent;
(c) the reported issue has been caused by third party software not provided by Confluent, including any Customer code; or
(d) Customer has not made reasonable efforts to install and implement in a timely manner all available Maintenance Release(s) for the installed version of Supported Software.

4. Customer Success Technical Architect - Platinum Only. As part of Platinum-level Support Services, Confluent shall provide a customer success technical architect resource ("CSTA") to your account. A Confluent CSTA helps customers align Confluent products to business needs, through general product knowledge and proactive engagement. Your CSTA can guide your technical roadmap and facilitate other services across Confluent, including product, support services, and professional services. As needed, your CSTA may engage other experts within Confluent to provide deeper product and use case expertise. Please note that a CSTA's responsibilities are to provide general product knowledge and do not encompass more detailed product expertise or implementation guidance provided through Confluent Professional Services.

The following are representative responsibilities of the CSTA:

- Driving efficient application of purchased Confluent services - e.g. training, professional services and support
- Quarterly technical reviews
- Bi-weekly, remote office hours to discuss topics related to:
  - Project management

  - Development of Confluent Platform-related components
  - Architecture and configuration choices
  - Best practices for Confluent Enterprise monitoring, automation and integrations
  - Upgrade and migration planning
- Keeping your team informed and up to speed on product releases and recommending the best solutions for your needs
- Facilitates delivery of detailed postmortem reports following production incidents
- Serving as your voice within Confluent, including lobbying for your roadmap priorities

If you purchase both Premier Support for Confluent Cloud and Platinum-level Support Services for Confluent Platform, Confluent will provide a CSTA resource to perform the responsibilities described above, and the meeting frequency described above will be inclusive of both Cloud and Confluent Platform (i.e., the meetings will be consolidated, not duplicated).

5. **Extended Support - Platinum Only.** As part of Platinum-level Support Services, Confluent will provide extended Support Services ("Extended Support") for Supported Software for one additional year from the date of general availability (i.e., for 3 years from the date of general availability rather than for 2 years as specified in the Supported Versions and Interoperability document). Extended Support is subject to the following conditions:

   - Customer must install the most recent available Maintenance Release for the applicable version of Supported Software.
   - Confluent will provide code fixes as a cumulative patch. Each new code fix will be built upon all other code fixes available for the release.
   - Code fixes will be limited in scope, with priority given to fixes without Workarounds that are related to either security, data loss, or stability.
   - Extended Support is limited to use cases and deployments of Supported Software existing as of the end of the standard 2-year support window, and will not include support for new deployments, or new use cases of existing deployments, that use versions of Supported Software in the extended support window.

6. **Health+ (previously "Proactive Support")**. Health+ is a product available for Confluent Platform 6.0 and later that provides customers with intelligent alerts, monitoring dashboards, and an accelerated support experience for their Confluent Platform deployment. Health+ uses a "Telemetry Reporter" enabled by customers and configured on each Confluent Platform service to regularly send telemetry data to Confluent servers for storage and aggregation. Please see https://www.confluent.io/moreinformation/ to learn more about Confluent's data collection protocols for Health+.

7. **US-Only Support for Public Sector Customers.** Where Customer is a part of (or is working directly in support of) a U.S. federal, state, or local government, and "US-Only Support" is specified in the applicable Order, Confluent Support team personnel providing Support Services via the Support Portal will be U.S. Citizens, and the Support Portal and data submitted to Confluent via the Support Portal will be hosted within the United States. Customer acknowledges such localization may impact Confluent's ability to respond to Support Requests within the Target First Response Time, depending on when such requests are issued. Resolution of certain Issues may require participation of non-U.S. citizen personnel outside the Confluent support organization or the Support Portal; Confluent will make reasonable efforts to notify Support Portal users in such situations. Customer is prohibited from submitting information or data subject to specific controls or dissemination restrictions (e.g., CUI, ITAR/EAR information) to Confluent, and Customer is responsible for redacting all such information when submitting Support Requests and related information.

8. **Changes to Support Services.** This Support Services Policy may be updated from time to time in Confluent's sole discretion, provided that any such updates will not materially reduce the level of Support Services during Customer's applicable Order term. Any material changes to this Support Services Policy will not apply unless and until such changed terms are accepted by the Customer.

Exhibit 1:
Confluent Professional Services Description

Confluent or one of its third-party subcontractors may provide Confluent Services under the Contract. This Professional Services Description governs the delivery of Confluent Services in addition to the Contract.

1. Definitions.

1.1 **"Confluent"** means Confluent Federal, LLC and/or its affiliates.

1.2 **"Confluent Services"** means professional and advisory services provided by Confluent or its subcontractor(s) as specific engagements, pursuant to an applicable Order and as may be further described in an SOW.

1.3 **"Customer"** means the entity purchasing Confluent Services.

1.4 **"Contract"** means the contract or other agreement between Customer and Contractor for the purchase and delivery of Confluent Services.

1.5 **"Contractor"** means the entity from which Customer purchases Confluent Services.

1.6 **"Order"** means an agreement under the Contract for specified Confluent Services.

1.7 **"Services Materials"** means all materials provided to Customer in the course of the Confluent Services.

1.8 **"SOW"** means a statement of work setting out the scope of Confluent Services, including any assumptions and Customer obligations.

2. Delivery.

2.1 **Scheduling**. Prior to the delivery of Confluent Services, Confluent and Customer shall agree on a delivery schedule. Except as agreed to in writing, Confluent Services will be scheduled and delivered during Confluent's standard business hours, Monday through Friday, excluding Confluent, Customer, and public holidays ("Business Hours"). For Confluent QuickStart services, Confluent's ability to provide QuickStart services and any outcome is subject to the requirements set forth in the applicable readiness form and any other reasonable requirements.

2.2 **Rescheduling**. Customer may reschedule an engagement subject to agreement in writing, based on Confluent's discretion and availability. If causes outside of Confluent or Customer's reasonable control require that an engagement be rescheduled, Confluent and Customer will agree in good faith on a mutually acceptable rescheduled date.

2.3 **Billing**. Customer is responsible for payment for all Confluent Services listed in an Order. Confluent Services scheduled on an hourly basis are billed hourly. Increments of hours are rounded up to the hour. For Confluent Services scheduled on a daily basis, a "day" is one business day consisting of up to eight (8) hours, and Confluent Services are billed in days.

2.4 **Cancellation**. If scheduled Confluent Services are canceled by Customer on fewer than ten business days' notice prior to delivery, (including same-day or partial cancellation of scheduled days/hours), Customer may be charged any nonrefundable fees or travel expenses.

2.5 **Expiration**. Confluent Services not scheduled and delivered within one (1) year from Order acceptance (or other period specified in the Order) will expire unless otherwise agreed in writing.

2.6 **Location and Connectivity.** Except as otherwise set forth in an Order or SOW, Confluent Services will be provided remotely, at Customer's location specified in the Order, or such other location mutually agreed in writing. Confluent will make remote conferencing arrangements through a provider of Confluent's choice. Confluent will make reasonable efforts to accommodate requests for alternative remote conferencing arrangements with advance notice.

2.7 **Customer Obligations.** Except as otherwise set forth in an SOW, Customer will reasonably and in good faith cooperate with Confluent in connection with delivery of Confluent Services, including but not limited to:

2.7.1 Provide resources and assistance in a timely manner, including full access to relevant functional, technical, and business resources with adequate skills and knowledge to support the performance of the Confluent Services;

2.7.2 Respond timely to Confluent's communications;

2.7.3 Upon or prior to the commencement of Confluent Services, provide all applicable documentation of requirements, designs, and constraints, as well as access to all offices and computer systems reasonably required by Confluent to undertake the Confluent Services;

2.7.4 Assign an individual for each SOW with the authority to make decisions and who will be the primary point of contact for Confluent during provision of Confluent Services;

2.7.5 Manage all schedules and dependencies for Customer stakeholders and teams;

2.7.6 Provide access to, and share Customer's information with, Customer's vendors, affiliates, and agents for the purpose of providing Confluent Services; and

2.7.7 Obtain necessary consents, authorizations, and license rights including third party license rights required for Confluent to perform Confluent Services. Contractor will not be responsible for any deficiency or delay in performing Confluent Services if such deficiency or delay results from Customer's failure to fulfill its obligations.

3. [RESERVED]

4. Intellectual Property Rights in Services Materials. Confluent or its licensors own and shall retain all rights, title and interest, including but not limited to all patent, copyright, trade secret, know-how, design rights, trademark, and other intellectual property rights, in and to the Services Materials, including techniques, knowledge or processes, and any changes and other modifications thereto. The Services Materials are "commercial computer software" and shall be subject solely to the terms of the license in this Section, as specified in 48 C.F.R. 12.212 (or, where Customer is part of the U.S. Department of Defense, 48 C.F.R. 227.7202-2) and its successors. Confluent grants Customer a limited, non-exclusive, non-sublicensable, non-transferable license to use Services Materials solely in connection with Customer's use of Confluent's proprietary products for Customer's own business operations. Confluent reserves all rights not expressly granted herein. No rights are granted by implication. Notwithstanding anything to the contrary herein, Confluent and its personnel shall be free to use and employ its and their general skills, know-how, and expertise, and to use, disclose, and employ any generalized ideas, concepts, know-how, methods, techniques, or skills gained or learned during the course of performing Confluent Services hereunder. Notwithstanding any failure to so designate them, the Services Materials shall be Confluent's Confidential Information.

5. Warranties.

5.1 **Warranty**. Contractor represents and warrants that it shall deliver the Confluent Services in a professional manner consistent with industry standards; no warranty shall apply if the alleged warranty breach is caused by a modification by Customer or caused by third party software. Customer must provide Contractor written notification of any alleged breach of any warranty for Confluent Services within thirty (30) days following the performance of the applicable Confluent Services, with a precise description of the problem and all relevant information reasonably necessary to rectify a warranty breach. Contractor's entire obligation and Customer's sole and exclusive remedy for a breach of warranty will be for Contractor to re-perform the non-conforming Confluent Services.

5.2 **Disclaimer**. EXCEPT FOR THE WARRANTIES STATED IN THIS SECTION OR IN THE CONTRACT, NO OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, APPLY WITH RESPECT TO CONFLUENT SERVICES OR SERVICES MATERIALS. NOTWITHSTANDING THE FOREGOING, ANY CONFLUENT SERVICES PROVIDED AT NO CHARGE ARE PROVIDED "AS-IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND. NEITHER CONTRACTOR NOR CONFLUENT WARRANTS ERROR-FREE SERVICES OR THAT CONFLUENT WILL CORRECT ALL NON-CONFORMITIES.

CONFLUENT

CONFLUENT CLOUD SERVICES AGREEMENT FOR U.S. PUBLIC SECTOR

This Confluent Cloud Services Agreement for U.S. Public Sector ("Agreement") between **Confluent Federal, LLC** ("Confluent") and the purchaser or user ("Customer") of the Cloud Service, Support Services, and/or any professional and education services ("Confluent Offerings") governs the use of such Confluent Offerings where Customer is a part of a federal, state, or local government within the United States. The effective date of this Agreement ("Effective Date") is the effective date of the relevant Order or agreement providing for the use of the Confluent Offerings. By ordering Confluent Offerings governed by this Agreement, Customer is agreeing to and accepting the terms of this Agreement. You represent and agree that you have the legal authority to bind the government entity or agency on whose behalf you are accepting this Agreement, and the rights granted under this Agreement are expressly conditioned upon such authority. If Customer does not accept the terms of this Agreement, then Customer cannot use the Confluent Offerings.

1. CONFLUENT CLOUD SERVICE

1.1 Provision of the Cloud Service. The Cloud Service is licensed and not sold. During the applicable Order term, Confluent will: (a) make the Cloud Service available to Customer for Customer to access and use the Cloud Service in accordance with the terms of this Agreement, the Order, and the Documentation; (b) provide purchased Support Services to Customer at the level subscribed to by the Customer; (c) provide the Cloud Service in accordance with the applicable Service Level Agreement; and (d) provide the Cloud Service in accordance with all laws applicable to Confluent's provision of the Cloud Service generally.

1.2 Registration. Customer must register and set up an account to use the Cloud Service. Customer must keep the registration information accurate and complete. Customer is responsible for the security of its User IDs and passwords and for the use of its accounts and will immediately notify Confluent of any unauthorized use at support@confluent.io.

2. CUSTOMER USE

2.1 Acceptable Use; Additional Restrictions on Use. Customer shall comply with (and shall ensure its Users comply with) Confluent's Acceptable Use Policy. Customer shall not resell, sublicense, rent, lease or otherwise make the Cloud Service available to any third party, other than its Users. Customer shall not use the Cloud Service to threaten or violate the security or integrity of any network, computer, communications system, software application, or computing device. Customer shall not make network connections to any third-party users, hosts, or networks unless Customer has permission to make such connections and may not use manual or electronic means to avoid any use limitations placed on the Cloud Service, such as access and storage restrictions. Confluent may but has no obligation to (a) investigate any violation of this provision or misuse of the Cloud Service, or (b) remove any Content, or disable access to any resource, that violates this section 2.1, however Confluent will use reasonable efforts in the circumstances to provide Customer with prior notice and an opportunity to remedy such violation or threat.

2.2 Content Restrictions and Responsibilities. Customer shall not transmit Content that is illegal, fraudulent, infringing, or in violation of any individual's or privacy rights. Customer is solely responsible for (a) the legality of Content; (b) ensuring compliance with all laws applicable to the

collection and provision of Content; (c) its Users' compliance with this Agreement, Orders and Documentation; and (d) its configuration and use of the Cloud Service, including compliance with its obligations under the Security Addendum. To the extent that Customer is or becomes subject to user data access and deletion requests, Customer is solely responsible for configuring the retention period on Apache Kafka topics (i.e., category names to which messages are stored and published) that contain personal identifiable data in accordance with the requirements of any applicable data protection laws.

2.3 No Classified Content. Customer may not use any version of the Cloud Service (including Confluent Cloud for Government) to process or store classified Content. Direct damages under this Agreement include sanitization costs to remedy a spillage in violation of this restriction.

3. PRIVACY AND SECURITY. Each party shall comply with its obligations under the Data Processing Addendum, which is hereby incorporated by attachment. Confluent will use appropriate administrative, physical, and technical safeguards designed to prevent unauthorized access to, use or disclosure of Content, as more fully described in the Security Addendum. Confluent will not access any Content except to the extent necessary to provide the Cloud Service or Support Services, to enforce the provisions of this Agreement, or for a Permitted Disclosure (as defined in section 6.1).

4. ORDERS, FEES AND RELATED

4.1 Orders Generally. All Orders are subject to the terms of this Agreement and are not binding until accepted by Confluent. Orders created by Customer through the Confluent Cloud website are deemed accepted when Confluent provides access to the service environment selected by Customer.

4.2 Fees and Payment. Customer agrees to pay Confluent (or its authorized reseller, if applicable) all fees specified in an Order, including all fees incurred for its usage of the Cloud Service. Unless agreed otherwise in a written Order between the parties, Customer's use of the Cloud Service is subject to the fee schedule specified in the Confluent Cloud user interface, and usage fees will be calculated and billed monthly in arears.

4.3 Taxes. Vendor shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

4.4 U.S. Government Customers
Notwithstanding the foregoing, if Customer is an agency of the U.S. Government and is exempt from the transaction taxes stated above, Confluent or its authorized reseller, as applicable, shall separately state the transaction taxes on invoices, and Customer will either pay the amount of the taxes or provide evidence necessary to sustain an exemption.

4.4 Late Payments. This Section 4.4 shall only apply if Customer is not an agency of the U.S. Government. Without limiting Confluent's rights or remedies, late payments may accrue interest at the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

4.5 Payment Disputes. Where applicable, Confluent will not exercise its rights under the "Late Payments" section above if Customer is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.

4.6 Marketplace Orders. For the avoidance of doubt, where Customer places an Order through a third-party Marketplace, Orders are subject to this Agreement and the applicable Marketplace Platform Provider's terms. Fees will be as specified in an Order and/or Confluent cloud user interface, as applicable, and will be payable to the Marketplace Platform Provider.

4.7 Indirect Orders. For the avoidance of doubt, where Customer purchases the Cloud Service through a Confluent-authorized reseller, Customer's payment obligations are owed to the reseller for such purchase and different or additional terms as agreed between Customer and Reseller may apply.

5. INTELLECTUAL PROPERTY OWNERSHIP

5.1 Confluent Materials. Confluent or its licensors retain all rights, title and interest, in and to all intellectual property rights in the Cloud Service, including all related and underlying technology and Documentation, any other materials provided by Confluent relating to the Cloud Service, and any derivative works, changes, corrections, bug fixes, enhancements, updates, modifications, or improvements of any of the foregoing ("Modifications") (collectively, "Confluent Materials"). Except for the express limited rights set forth under this Agreement, no right, title or interest in any Confluent Materials is granted to Customer. Customer acknowledges that the licenses granted in this Agreement do not include the right to prepare any Modifications of the Confluent Materials. Confluent reserves all rights not expressly granted in this Agreement.

5.2 Content. Except for the limited rights granted under this Agreement, as between Customer and Confluent, Customer retains all rights, title and interest, including all intellectual property rights, in Content.

5.3 Feedback. Customer has no obligation to provide Confluent any suggestions, enhancement requests, recommendations, or other feedback regarding Confluent's products and services ("Feedback"). However, Confluent may use and include any Feedback that Customer provides regarding Confluent's products and services without restriction or payment. Confluent acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

6. CONFIDENTIALITY

6.1 Confidentiality Obligations. Each party shall retain in confidence the non-public information and know-how disclosed or made available by the other party pursuant to this Agreement which (a) is designated in writing as proprietary and/or confidential, if disclosed in writing, (b) if disclosed orally, is designated in writing (which may be via email) as confidential within thirty (30) days of the oral disclosure, or (c) should reasonably be understood to be confidential by the recipient ("Confidential Information"). Notwithstanding any failure to so designate it, Confidential Information of Confluent includes the Cloud Service, and all Orders hereunder, and Content is Customer's Confidential Information. Each party shall (x) maintain the confidentiality of the other party's Confidential Information using the same degree of care that it uses to protect the confidentiality of its own similar

Confidential Information and at least a reasonable degree of care; (y) refrain from using the other party's Confidential Information except for the purpose of performing its obligations under this Agreement; and (z) not disclose Confidential Information to any party except to its and its Affiliate's employees, subcontractors, and agents as is reasonably required in connection with this Agreement, and who are subject to confidentiality obligations at least as protective as those set forth in this section. The foregoing obligations will not apply to Confidential Information of the other party which (i) is or becomes publicly known without breach of this Agreement; (ii) is discovered or created by the receiving party without use of, or reference to, the Confidential Information of the disclosing party, as shown in records of the receiving party; or (iii) is otherwise known to the receiving party without confidentiality restrictions and through no wrongful conduct of the receiving party. Receiving party may disclose Confidential Information to the extent required by law or court order (including where Customer is the receiving party and is subject to the U.S. Freedom of Information Act (5 U.S.C. 552) or similar public or open records law) if the receiving party provides prompt notice and reasonable assistance to the disclosing party to enable the disclosing party to seek a protective order or otherwise prevent or restrict such disclosure ("Permitted Disclosure"); and provided that any information so disclosed retains its confidentiality protections for all other purposes.

6.2 Reserved.

7. WARRANTIES AND DISCLAIMERS

7.1 Mutual Warranties. Each party represents and warrants to the other that it has full corporate right and authority to enter into and perform this Agreement.

7.2 Confluent Warranties. Confluent represents and warrants that (a) it shall perform Support Services in a professional manner, employing a standard of care, skill, and diligence consistent with industry standards, (b) the Cloud Service will perform in all material respects in accordance with the applicable Documentation and (c) Confluent will not materially decrease the overall security of the Cloud Service during the applicable Order term. Confluent's entire obligation and Customer's sole remedy for a breach of the foregoing warranties will be for Confluent to re-perform the Support Services in accordance with the requirements stated in the Support Services terms, or to correct any nonconformity in the Cloud Service, as applicable. The foregoing warranties will not apply unless Confluent is notified in writing of the applicable nonconformity within thirty (30) days of the date on which Customer first became aware of such applicable nonconformity.

7.3 Customer Warranties. Customer warrants that (a) any use of the Cloud Service or Content in connection with the Cloud Service will not violate the acceptable use and Content restrictions under Section 2; (b) that Content (or combinations of Content with other data or content), including any use, development, or design of the foregoing will not infringe or misappropriate the rights of any third party; and (c) use of the Cloud Service will not cause harm to any third party.

7.3 Warranty Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS AGREEMENT, CONFLUENT MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE CLOUD SERVICE, SUPPORT SERVICES OR ANY OTHER CONFLUENT MATERIALS OR SERVICES PROVIDED HEREUNDER. UNLESS CONTRARY TO APPLICABLE LAW, CONFLUENT SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE,

FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. CONFLUENT DOES NOT WARRANT THAT THE CLOUD SERVICE WILL OPERATE UNINTERRUPTED OR ERROR FREE, OR THAT ALL ERRORS WILL BE CORRECTED.

8. INDEMNIFICATION

8.1 By Confluent. Confluent will have the right to intervene to defend Customer from and against any claim, demand, or lawsuit brought against Customer by a third party alleging that the Cloud Service provided under an Order, as made available to Customer by Confluent and used pursuant to this Agreement, infringes such third party's intellectual property rights, and Confluent will pay such damages and/or costs as are finally awarded against Customer or agreed to in settlement attributable to any such action, provided that Customer gives Confluent (a) notification in writing of any such action within sixty (60) days of Customer's receipt thereof; (b) sole control of the defense or settlement of such action (provided any settlement releases Customer from all liability), except as prohibited by 28 U.S.C. 516, in which case Customer will consult with Confluent regularly during such action and Confluent will retain the right to intervene in the proceedings at its own expense, through counsel of its choice; and (c) all reasonable information and assistance, at Confluent's expense. If the Cloud Service becomes, or in the opinion of Confluent is likely to become, the subject of such an infringement claim, Confluent shall, at its option and expense, either: (i) procure for Customer the right to use the allegedly infringing element of the Cloud Service, at no charge to Customer; (ii) replace or modify, in whole or in part, the Cloud Service to make it non-infringing; or (iii) if neither (i) or (ii) are commercially available, terminate the applicable Order, and refund a pro rata portion of any fees pre-paid by Customer for the terminated Cloud Service. Confluent assumes no liability hereunder for any claim of infringement if such claim is based on: (a) Content, (b) the combination, operation or use of the Cloud Service, with non-Confluent programs or hardware, if the claim would not have arisen but for such combination, operation or use, (c) the open source versions of Apache Kafka or Apache Flink, or any other third party software, or (d) use of the Cloud Service other than in accordance with this Agreement and Documentation. THIS SECTION SETS FORTH CONFLUENT'S ENTIRE LIABILITY AND OBLIGATION AND CUSTOMER'S SOLE REMEDY FOR ANY CLAIM OF INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS. If Customer is a party of the U.S. Government and written approval of the Attorney General is required for Customer to accept the above procedures, Confluent will defend and indemnify Customer as described above only upon such approval.

8.2 Reserved.

9. LIMITATION OF LIABILITY

9.1 NOTHING IN THIS AGREEMENT LIMITS EITHER PARTY'S (I) LIABILITY FOR PERSONAL INJURY, DEATH OR WILLFUL MISCONDUCT, (II) LIABILITY THAT CANNOT BE LIMITED BY APPLICABLE LAW, (III) LIABILITY FOR BREACH OF SECTION 6 (CONFIDENTIALITY) (EXCEPT FOR ANY CLAIMS OR LIABILITY RELATED TO CONTENT, WHICH SHALL BE SUBJECT TO SECTION 9.3 BELOW), (IV) OBLIGATIONS UNDER SECTION 8 (INDEMNIFICATION); OR (V) LIABILITY FOR BREACH OF SECTION 2.3 (NO CLASSIFIED CONTENT).

9.2 EXCEPT AS SET FORTH IN SECTION 9.1, IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EITHER PARTY TOGETHER WITH ALL OF ITS AFFILIATES EXCEED THE TOTAL AMOUNT PAID OR PAYABLE BY

CUSTOMER AND ITS AFFILIATES TO CONFLUENT UNDER THIS AGREEMENT FOR THE SERVICES GIVING RISE TO THE LIABILITY DURING THE TWELVE (12) MONTHS IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY.

9.3 NOTWITHSTANDING ANYTHING TO THE CONTRARY IN 9.2, CONFLUENT'S AGGREGATE LIABILITY FOR ITS FAILURE TO COMPLY WITH ITS OBLIGATIONS UNDER SECTION 3 (PRIVACY AND SECURITY), SHALL NOT EXCEED TWO TIMES (2X) THE AMOUNT OF FEES PAID BY CUSTOMER UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

9.4 NEITHER PARTY NOR ITS AFFILIATES WILL BE LIABLE TO THE OTHER PARTY UNDER THIS AGREEMENT FOR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, INDIRECT, PUNITIVE OR EXEMPLARY DAMAGES OF ANY KIND, OR FOR LOSS OF BUSINESS, PROFITS, GOODWILL, ANTICIPATED SAVINGS, OR DATA, OR FOR ANY CLAIM OR DEMAND BY ANY OTHER PARTY, HOWEVER CAUSED, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY.

THESE EXCLUSIONS AND LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

10. TERM AND TERMINATION

10.1 Agreement Term. This Agreement commences on the Effective Date and will remain in effect until terminated as provided below.

10.2 Service Term. The Subscription Term for the Cloud Service shall be set out in the applicable Order. Customer may discontinue its use of the Cloud Service at any time for any reason by following the process in the Confluent website interface to "Delete" Customer's purchased Cloud Service. Discontinuing use of the Cloud Service will not relieve Customer of any incurred fees and committed payment obligations through the end of all applicable Orders, nor entitle Customer to a refund of any pre-paid amounts.

10.3 Termination for Cause. RESERVED

10.4 Effect of Termination. Termination or expiry of an Order will not automatically result in termination of this Agreement. The provisions of this Agreement that by their nature extend beyond the termination of this Agreement including without limitation "Orders", "Fees and Related", "Intellectual property Ownership", "Confidentiality", "Indemnification", "Limitation of Liability" and "Term and Termination" will survive termination. Upon termination of this Agreement, Customer will immediately cease use of and access to the Cloud Service and the Support Services. Customer is solely responsible for exporting Content from the Cloud Service prior to discontinuation or termination of its use of the Cloud Service.

11. TRIAL USAGE. "Trial Usage" is a short-term evaluation of the Cloud Service that is (i) provided free of charge or discounted due to Customer receiving from Confluent one or more coupon codes or credits towards such usage, or (ii) pursuant to an Order that is specifically labeled "Proof of Concept."

A Trial Usage period ends the earlier of (a) the date Customer enters into a commitment Order for the Cloud Service for a minimum one-year term, or (b) the date Customer has paid non-discounted rates for a period of at least three consecutive months after all coupons expire. For clarity, if more than one coupon code or credit is provided to Customer, Customer's usage will be considered Trial Usage throughout any interim period between coupon codes or credits. The terms of this section 11 govern Trial Usage and control over any conflicting provision of this Agreement; provided however that Trial Usage will be subject to all applicable provisions of this Agreement that are not in conflict with the provisions of this section 11. Trial Usage shall be limited to internal testing and evaluation purposes on a development or non-production cluster. Unless specifically stated otherwise in an Order, Trial Usage is provided: (a) without support; (b) "AS IS"; and (c) without indemnification, warranty, or condition of any kind. No service level commitment will apply to Trial Usage. Customer must not transmit production data or data regulated by law or regulation into the Cloud Service during Trial Usage. Certain features or functionality of the Cloud Service may not be available in Trial Usage.

12. GENERAL

12.1 Assignment. Neither party may assign or otherwise transfer this Agreement or any rights or obligations hereunder, in whole or in part, whether by operation of law or otherwise, to any third party without the other party's prior written consent, except to an Affiliate or to any successor to its business or assets to which this Agreement relates, whether by merger, sale of assets, sale of stock, reorganization or otherwise. Any purported transfer, assignment or delegation without such prior written consent will be void. Confluent may not perform any assignment under this Agreement that violates the Anti-Assignment Act, 41 U.S.C. 6305. Subject to this section, this Agreement shall be binding upon and inure to the benefit of the parties, and their respective successors and permitted assigns.

12.2 Delays. In accordance with FAR Clause 52.212-4(f), In the event that either party is unable to perform any of its obligations under this Agreement due to any Act of God, fire, casualty, flood, earthquake, war, strike, lockout, epidemic, destruction of production facilities, riot, insurrection, material unavailability, acts or intervention of governmental authority, or any other cause beyond the reasonable control of the party invoking this section, and if such party used its commercially reasonable efforts to mitigate its effects, such party shall give prompt written notice to the other party, and the time for the performance shall be extended for the period of delay or inability to perform due to such occurrences.

12.3 Governing Law. This Agreement is governed by the Federal laws of the United States (or, if Customer is a part of a state or local government, the laws of that state). The parties disclaim and exclude the application of the United Nations Convention on Contracts for the International Sale of Goods.

12.4 Export Compliance. Confluent Materials are subject to export control laws and regulations. Customer may not access or use the Confluent Materials or any underlying information or technology except in full compliance with all applicable United States export control laws. Neither the Confluent Materials nor any underlying information or technology may be accessed or used (a) by any individual or entity in any country to which the United States has embargoed goods; or (b) by anyone on the U.S. Treasury Department's list of specially designated nationals or the U.S. Commerce Department's list of prohibited countries or debarred or denied persons or entities.

12.5 Government End-Users. The Cloud Service and Confluent Materials are developed at private expense, and are licensed to the U.S. Government as "commercial items," "commercial computer software," "commercial computer documentation," and "technical data," as those terms are defined in 48 C.F.R. Ch 1 ("FAR") and 48 C.F.R. Ch. 2 ("DFARS"). Customer agrees that the Cloud Service, Support Services, and professional and educational services are commercial products and commercial services under FAR 2.101. Any use, modification or disclosure of the foregoing is subject solely to the terms of this Agreement and any other restrictions that generally apply to the Cloud Service and Confluent Materials.

12.6 Other. This Agreement, together with and inclusive of any referenced exhibits, addenda and any incorporated terms, represents the entire agreement between the parties, and supersedes all prior agreements and understandings, written or oral, with respect to its subject matter, and is not intended to confer upon any third-party any rights or remedies. Customer acknowledges that it has not relied on any representations other than those contained in this Agreement. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, shall be effective unless in writing and signed by both parties. In the event of a conflict between the terms of this Agreement and an Order, the terms of the Order shall prevail. The terms of this Agreement will supersede any additional or conflicting term in any other purchasing-related document issued by Customer and relating to an Order. The waiver of one breach or default or any delay in exercising any rights will not constitute a waiver of any subsequent breach or default. If any provision of this Agreement is held invalid or unenforceable under applicable law by a court of competent jurisdiction, it will be replaced with the valid provision that most closely reflects the intent of the parties and the remaining provisions of this Agreement will remain in full force and effect. Confluent may use and display Customer's name and logo on the Confluent website and in Confluent marketing and sales materials for the Cloud Service. Nothing in this Agreement will be construed as creating an agency, partnership, or joint venture relationship between the parties. Neither party shall have any right or authority to assume or create any obligations or to make any representations or warranties on behalf of the other party, whether express or implied, or to bind the other party in any respect. Confluent will provide any required notice to Customer under this Agreement by sending the notice by email to the email address that Customer provides to Confluent for its account. To provide notice to Confluent under this Agreement, Customer must send the notice, expressly referencing this Agreement and section with respect to which Customer is providing notice, by email to legal@confluent.io.

13. MARKETPLACE TERMS. The following terms apply solely to Orders placed through the Marketplace.

13.1 Cloud Service Commencement Date. In certain scenarios, the commencement date of the Cloud Service may be up to several days later than the date of the Order.

13.2 Reporting Times. Reporting time on metered billing will be shifted by several hours to accommodate varying reporting requirements by the applicable Marketplace.

13.3 Renewals. Any Orders subject to discounts and Rate Cards will not automatically renew, regardless of whether Customer has checked a "renew" or auto-renewal box on the applicable Marketplace.

14. DEFINITIONS

14.1 “Acceptable Use Policy” means Confluent’s Acceptable Use Policy attached hereto and located at https://www.confluent.io/contracts/.

14.2 “Affiliate” means any entity that controls, is controlled by, or is under common control with a party, where “control” means direct or indirect ownership of more than 50% of the voting interests of the entity.

14.3 “Cloud Service” means the online, hosted and managed service for the processing of Content that Confluent makes available for Customer’s use, as described in the Documentation.

14.4 “Confluent Cloud for Government” means the FedRAMP-authorized version of the Cloud Service.

14.5 “Content” means all data and information submitted to the Cloud Service by Customer or on Customer’s behalf.

14.6 “Data Processing Addendum” means the agreement attached hereto and located at https://confluent.io/cloud-customer-dpa between Confluent and Customer.

14.7 “Documentation” means the published documentation describing the functionality of the Cloud Service, attached hereto and located at https://docs.confluent.io/cloud/current/overview.html.

14.8 “Marketplace” means the third-party platform through which Customer orders the Cloud Service or other services.

14.9 “Order” means: (a) an ordering document for a Cloud Service, Support Services, and/or any professional and training services, agreed upon by the parties and referencing this Agreement, or (b) the Cloud Service(s) selected and activated by Customer via the Confluent Cloud website, including any selected Support Services.

14.10 “Platform Provider” means the Marketplace vendor with which Customer places the Order.

14.11 “Security Addendum” means the Confluent Cloud Security Addendum attached hereto and located at https://confluent.io/cloud-enterprise-security-addendum.

14.12 “Service Level Agreement” means the uptime service level agreement attached hereto and as set forth at https://www.confluent.io/confluent-cloud-uptime-sla.

14.13 "Support Services" means the applicable support services that Customer purchases for the Cloud Service, as more fully described at https://www.confluent.io/confluent-cloud/support.

14.14 "User” means any person that Customer allows access to or use of the Cloud Service, and may include Customer's employees, contractors, service providers, and other third parties that use the Cloud Service in connection with Customer’s own business operations.

CONFLUENT FEDERAL, LLC.	**CUSTOMER**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

CONFLUENT

Confluent's Cloud Security Addendum ("Security Addendum") outlines the technical and procedural measures that Confluent undertakes to secure the Cloud Service. Confluent may update this Security Addendum from time to time and such changes will be effective when posted. Any material changes to this Security Addendum will not apply unless and until such changed terms are accepted by the Customer. Capitalized terms used but not defined in this Security Addendum have the meanings as set forth in the Confluent Cloud Services Agreement or other written or electronic terms of a cloud service or cloud subscription agreement ("Agreement") entered into by the parties. In the event of any conflict between the terms of the Agreement and this Security Addendum, this Security Addendum shall govern.

1. Confluent Information Security Program Overview

1.1 General Overview. Confluent is committed to achieving and maintaining the trust of its customers. Integral to this mission is providing a robust security that carefully considers data security matters across the Cloud Service, including security of Content. To this end, Confluent maintains a comprehensive documented information security program to establish and maintain administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, availability, and security of the Cloud Service and Content ("Information Security Program"). Confluent is regularly audited by accredited third parties and has achieved various compliance standards and certifications covering the Information Security Program, including:

1.1.1 SSAE 21 SOC 1 Type II, SOC 2 Type II, and SOC 3;

1.1.2 HITRUST CSF Certification;

1.1.3 Payment Card Industry Data Security Standards ("PCI-DSS") – Confluent can support PCI data that is message-level encrypted by Customer;

1.1.4 CSA Star Level 2 Attestation; and

1.1.5 ISO 27001 and 27701 Certifications.

Confluent's Trust and Security page (https://www.confluent.io/trust-and-security) provides detailed information about Confluent's compliance certifications and a portal for requesting supporting documentation.

1.2. Maintenance and Compliance. Confluent's Information Security Program is maintained by a security team, led by Confluent's Chief Information Security Officer. Confluent monitors compliance with its Information Security Program and conducts ongoing education and training of personnel to ensure compliance. The Information Security Program is reviewed and updated at least annually to reflect changes to Confluent's organization, business practices, technology, services, and applicable laws and regulations; provided, however, Confluent will not update the Information Security Program in a way that materially degrades the overall security of the Cloud Service.

2. Storage Location of Message Content

2.1 Storage Location. For Content that consists of message data produced to a Kafka topic ("Message Content"), Customer determines, via configuration in the Cloud Service, the Cloud Service region where the Message Content is stored.

3. Encryption

3.1 Encryption at Rest. The Cloud Service stores Content encrypted at rest. This is done leveraging enterprise grade encryption standards employed on the storage backend using AES-256 bit, or the equivalent or better.

3.2 Encryption in Transit. Communications between Customer's endpoints and the Cloud Service are encrypted in-transit with appropriate encryption standards for data in motion using TLS v.1.2 or higher.

4. Systems and Network Security

4.1 Separation of Content. The Cloud Service maintains logical separation of Content between customers. Confluent has implemented controls to prevent one

customer from gaining unauthorized access to another customer's data in the Cloud Service.

4.2. Access Management

4.2.1 Access Controls. Access to the systems and infrastructure that support the Cloud Service is granted solely to individuals whose job responsibilities require it. Role separation with different levels of access is enforced to adhere to the principle of least privilege.

4.2.2 Access Authentication. Confluent personnel can access the Cloud Service only through their Confluent provisioned and managed endpoints. Additionally, such Confluent personnel access the Cloud Service via unique user IDs and MFA. The password policy for the Cloud Service adheres to industry-standard complexity rules. Access to infrastructure components of the Cloud Service takes place via authenticated and encrypted connections such as SSH with certificate-based keys, and never only passwords.

4.3 Firewall. Cloud provider firewall or firewall-equivalent controls have deny-all default policies and only enable appropriate network protocols for ingress network traffic. Egress network traffic patterns are subject to monitoring for security purposes, with any identified events promptly addressed.

4.4 Vulnerability Management and Remediation

4.4.1 Vulnerability Management. Vulnerability mitigation is a part of every Confluent engineer's responsibilities. Confluent maintains secure software development life cycle practices to protect and to address security vulnerabilities in the Cloud Service. Confluent's security team continuously evaluates the impact of security advisories and vulnerabilities in commercial and open-source software based on Confluent-defined risk criteria, including applicability and severity.

4.4.2 Vulnerability Remediation. Confluent addresses vulnerabilities confirmed to impact confidentiality, integrity, or availability of the Cloud Service in accordance with industry standard SLAs, including using reasonable tracking mechanisms and risk management practices. Confluent will use commercially reasonable efforts to

address security updates rated as “high” or “critical” within thirty (30) days of the patch release and “medium” with ninety (90) days of the patch release. To determine whether a security update is “critical”, “high” or “medium”, Confluent utilizes the National Vulnerability Database’s Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-CERT rating.

4.5 Penetration Tests. Penetration tests by independent third parties are conducted at least annually. Detailed results from external penetration tests are not distributed or shared with anyone other than Confluent employees with a need to know; provided, however, redacted summaries are available per Section 1.1.

4.6. Secure Systems Operation and Maintenance. For Confluent-managed systems that process Content, Confluent meets or exceeds industry standards to ensure secure operations. This includes, without limitation, software integrity checks, operating system vulnerability scanning, and periodic patching through the rolling of infrastructure components of the Cloud Service to newer versions as they become available by cloud service providers.

4.7. Infrastructure Event Logging. Monitoring tools and services are used to monitor the infrastructure including network, availability events, resource utilization, and other operational events of interest. Security events of interest identified by Confluent in the Cloud Service are reviewed for malicious or inappropriate activity. Confluent infrastructure event logs are collected in a central system and stored using appropriate security measures designed to prevent tampering. Logs are stored for at least twelve months.

5. Administrative Controls

5.1 Personnel Screening. To the extent permitted by applicable law, Confluent personnel undergo a background check as part of the hiring process. Such background checks include, at minimum, criminal convictions check, global sanctions check, education verification, and identity check, all to the extent permitted by applicable law.

5.2 Security and Privacy Training. Confluent maintains a security and privacy awareness program for Confluent personnel, which provides initial education,

ongoing awareness, and individual Confluent personnel acknowledgment of intent to comply with Confluent's corporate security and privacy policies. All Confluent personnel are required to satisfactorily complete security and privacy training annually.

5.3 Access Review. Confluent personnel access to the systems and infrastructure that support the Cloud Service is reviewed quarterly. Access privileges of terminated Confluent personnel are disabled promptly. Access privileges of persons transferring to jobs requiring reduced privileges are adjusted accordingly.

5.4 Storage of Content. Confluent maintains a policy of not storing Content on local desktops, laptops, mobile devices, shared drives, removable media, as well as on public facing systems that do not fall under the administrative control or compliance monitoring processes of Confluent.

5.5 Reporting. All Confluent personnel acknowledge they are responsible for reporting actual or suspected concerns, thefts, breaches, losses, and unauthorized disclosures of or access to Message Content.

5.6 Risk Management. Confluent maintains a risk management program based on industry standards. Confluent conducts risk assessments of various scope throughout the year, including self and third- party assessments and tests, automated scans, and manual reviews. Results of assessments, including formal reports, as relevant, are reported to the head of the Confluent Security Committee ("Security Committee"). The Security Committee meets biannually to review reports, to identify control deficiencies and material changes in the threat environment, and to make recommendations for new or improved controls and threat mitigation strategies to executive management. Changes to controls and threat mitigation strategies are evaluated and prioritized for implementation on a risk-adjusted basis. Threats are monitored through various means, including threat intelligence services, vendor notifications, and trusted public sources.

5.7 Third Party Risk Assessment. Confluent maintains and implements a third party risk management assessment program ("TPRM") for Subprocessors, as defined in the DPA. Confluent's TPRM assesses these Subprocessors to appropriately measure and manage risk. Confluent has entered into written agreements with its

Subprocessors containing privacy, data protection and data security obligations that provide a level of protection appropriate to the processing activities provided by them. Compliance with such obligations are subject to regular reviews.

6. Physical and Environmental Controls

6.1 Cloud Service Provider Data Centers. As further described in the DPA and Documentation, the Cloud Service is hosted in AWS, GCP, Azure, and other public clouds. Therefore, all physical security controls are managed by the applicable public cloud provider. Annually, Confluent reviews the applicable security and compliance reports of the public cloud providers it uses to ensure appropriate physical security controls, including:

6.1.1 Visitor management including tracking and monitoring physical access;

6.1.2 Physical access point to server locations are managed by electronic access control devices;

6.1.3 Monitor and alarm response procedures;

6.1.4 Use of CCTV cameras at facilities;

6.1.5 Video capturing devices in data centers with ninety days of image retention;

6.1.6 Environmental and power management controls; and

6.1.7 Removal and destruction of physical media including drives.

Information about security and privacy-related audits and certifications received by AWS, GCP, Azure, and Jio Cloud, including information on ISO 27001 and 27701 certifications and Service Organization Control (SOC) reports, is available as follows: For AWS, AWS Security Website and the AWS Compliance Website; for GCP, GCP Security Website and GCP Compliance Website; for Azure, Azure Security Website and Azure Compliance Website; and for Jio Cloud, JioCloud Data Security Website.

6.2 Confluent Corporate Offices. Confluent has implemented administrative, physical, and technical
safeguards for Confluent-managed corporate offices. These include, but are not limited to, the
following:

6.2.1 Physical access to Confluent-managed corporate offices are controlled at office ingress points;

6.2.2 Visitors are required to sign in and wear an identification badge;

6.2.3 Tagging and inventory of Confluent-issued laptops and network assets; and

6.2.4 Confluent corporate offices, including LAN and Wi-Fi networks in those offices, require successful authentication in addition to authentication to public cloud provider accounts for access.

7. Business Continuity and Disaster Recovery

7.1 Business Continuity and Disaster Recovery Plan. Confluent maintains a business continuity and disaster recovery plan ("BCDR Plan") for the Cloud Service. The BCDR Plan is tested at least annually. Customer is responsible for ensuring that it implements a service level that corresponds with Customer's business continuity and disaster recovery strategy. Each of the cloud platform providers, such as AWS, Azure, and GCP, offers inbuilt disaster recovery solutions, which Customer is responsible for employing as part of Customer's disaster recovery strategy.

8. Notification of Security Breach and Response

8.1 Security Breach Notification. Confluent will notify Customer in writing without undue delay, but no later than seventy-two (72) hours, of confirmed accidental or unlawful destruction, loss, or alteration, or unauthorized disclosure of, or access to, Message Content as a result of a breach of Confluent's security ("Security Breach").

8.2 Communication and Cooperation. The Security Breach notification will summarize the known details of the Security Breach and the status of Confluent's investigation. Where reasonably possible, Confluent will update Customer of the

Security Breach with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a future similar event.

8.3 Investigation and Mitigation. Confluent will take appropriate actions to contain, investigate, and mitigate any such Security Breach.

9. Shared Customer Responsibilities

9.1 Customer User Credentials. Customer controls access to the Cloud Service via unique user IDs and passwords ("User Credentials") or an integration with Customer's Identity Provider ("IDP"). Customer is responsible for managing and securing User Credential(s) within the Cloud Service and for protecting its own resources used to send Content to the Cloud Service. Customer will immediately notify Confluent if a User Credential has been compromised or if Customer suspects possible suspicious activities that could negatively impact the security of the Cloud Service or Customer's account.

9.2 Encryption. Customer is responsible for appropriately using the Cloud Service to ensure a level of data protection commensurate with the sensitivity of the Message Content it uploads to the Cloud Service including, without limitation, an appropriate level of message-level encryption.

9.3 Retention of Message Content. Message Content is replicated by Confluent and retained per Customer's specified retention periods set by Customer in the Cloud Service. Customers are expected to consume Message Content regularly and store Message Content in their data stores of choice for storage beyond the retention policy specified.

9.4 Backup of Message Content. Customer is responsible for managing a backup strategy regarding Message Content.

Confluent Cloud Definitions and Rules

Effective Date: February 2, 2026

These definitions and rules supplement and are incorporated by reference into Customer's applicable Order with Confluent. All capitalized terms will have the meanings assigned to them in the Order or the Agreement.

Confluent may update these definitions and rules from time to time. Any material changes to these definitions and rules will not apply unless and until such changed terms are accepted by the Customer. Each update will bear an Effective Date, and will apply only to Orders that are entered into after such Effective Date. Prior versions (available in the archive on confluent.io/contracts) remain applicable to Orders entered into during the effective period of such versions.

Pricing: Fees for the Cloud Service are based on per-unit pricing and are charged in accordance with Customer's usage of each component of the Cloud Service, as further described in Customer's Order.

Billing: Cloud Service bills are based on Customer's consumption of resources within Customer's Cloud Organization ID and Tenant ID. Billing for each Cloud Service component accrues at intervals set forth in the Rate Card. All billing computations are conducted in Coordinated Universal Time (UTC). To view billing information, log into the Cloud Service and visit the Billing & Payment screen.

Eligible Accounts: Only Cloud Service fees incurred under the account identified in Customer's Order will be eligible for any Discount outlined in the Order.

Total Available Balance: The amount of Cloud Service usage fees the Customer may consume prior to being billed overages during the Order Term.

Net Payable Amount: The amount the Customer is committed to pay under an applicable Order, subject to any schedule defined therein. If not stated, it shall be equivalent to the Total Available Balance.

Support and Additional Services: Confluent offers 3 levels of add-on Support Services plans for the Cloud Service: Developer, Business, and Premier. If Customer elects Premier-level Support Services, then (a) such Support Services must be maintained at the Premier level for the entire Order Term, and (b) following the Order Term, such Premier-level Support Services will end, unless Customer enters into a new commitment Order.

Except for the BYOC Service as set forth on the applicable Order, Support Services are optional and not eligible for any Discounts, but such fees will draw down from the Total Available Balance. Purchases of additional services such as professional services and education services are not subject to any Discount and will not draw down from the Total Available Balance. Confluent's Support Services offerings and monthly charges are described at https://www.confluent.io/confluent-cloud/support.

New Components and Continued Usage: If Confluent adds new features or components to the Cloud Service during an Order Term ("New Components") for which Confluent charges separate fees, Confluent will publish supplemented pricing to Customer's Rate Card on or before the date of general availability, and Customer will be charged for usage of such New Components in accordance with such pricing. Any Discount will not be applied to charges for the New Components during the Order Term. If such New Components are initially made available as "Preview" or "Early Access," the pricing may change when the New Components are made generally available.

Additional Terms for BYOC Service: Unless otherwise set forth in the applicable Order, pricing for the BYOC Service Rate Card is published at www.warpstream.com/pricing. Billing for each BYOC Service cluster accrues in 15-minute increments. The BYOC Service has only Business and Premier Support Service plans. In addition, the BYOC Service is subject to the Bring Your Own Cloud Service Terms set forth at https://www.confluent.io/contracts/.

Cloud Parent ID and Child Cloud Organization IDs: If set forth in an applicable Order, the Total Available Balance in the Cloud Parent ID will be shared across the Child Cloud Organization IDs listed on the applicable Order or other Child Cloud Organization IDs requested by Customer and approved by Confluent as set forth below. Any Cloud Service usage in a Child Cloud Organization ID will draw down against the Total Available Balance and billed in accordance with the Cloud Parent ID's Rate Card. Once the Total Available Balance is exhausted, Customer is responsible for all overages in each Child Cloud Organization ID, which Confluent will bill monthly in arrears. A "Child Cloud Organization ID" means a unique Confluent Cloud Organization ID attached to a Cloud Parent ID that is responsible for fees.

During the Order Term, Customer may create new Child Confluent Cloud Organization IDs to add to the applicable Order ("New Child OrgID") that may draw against the Total Available Balance, provided (i) Customer is in compliance with the terms of the Order, (ii) Customer has not reached the Total Available Balance, and (iii) the request is made at least two months prior to the end of the applicable Order Term. Customer's request will be processed within 30 business days. Adding a New Child OrgID does not extend the applicable Order Term.

Except as explicitly set forth in an applicable Order, each Child Cloud Organization IDs is charged the minimum fee for Support Services, including percentage based on usage.

Confluent Cloud Service Level Agreement

This Confluent Cloud Service Level Agreement ("SLA") describes the service availability commitment for the applicable Confluent Cloud Service purchased by Customer pursuant to the applicable agreement for the Cloud Service ("Agreement") between the Confluent entity which entered into the Agreement ("Confluent") and Customer. Unless otherwise provided herein, this SLA is subject to the terms of the Agreement and capitalized terms will have the meaning specified in the Agreement.

During Customer's use of the Cloud Service, Confluent will use commercially reasonable efforts to make the Cloud Service available within the applicable Service Level. If Confluent does not meet the Service Level, Customer may be eligible to receive a Service Credit as described below. Confluent may update the SLA from time to time; provided, however, updates to the SLA will apply only to Orders entered into after the effective date of any update.

General Terms

Definitions

- **"Downtime"** is defined for the applicable Cloud Service function in the Service Specific Terms below. Downtime does not include unavailability that results from any of the exclusions set forth below or in the Service Specific Terms. Partial minutes of unavailability will not be counted as Downtime. Confluent's monitoring system connects to the same endpoints that Customer uses.
- **"Monthly Uptime Percentage"** is defined for each applicable Cloud Service function in the Service Specific Terms below.
- **"Service Credit"** means the percentage of monthly fees attributable to Customer's spend for the applicable Cloud Service function, calculated in Service Specific Terms, and credited to the Cloud Service bills in accordance with the process described in this SLA.
- **"Service Level"** means the Monthly Uptime Percentage for the applicable Cloud Service function as detailed in the Service Specific Terms section below.

Service Credits

Service Credits are calculated as a percentage of the total monthly fees paid by Customer for unavailable Cloud Service function for the calendar month in which the applicable Cloud Service function does not meet the Service Level, in accordance with the schedule below.

Service Credits are not refundable and can only be used toward future billing charges. Confluent will apply any Service Credits against Customer's next billing charge. Service Credits are exclusive of any applicable taxes charged to Customer or collected by Confluent. Service Credits will not entitle Customer to any refund or other payment from Confluent. Service Credits are Customer's sole and exclusive remedy for any unavailability of the Cloud Service in accordance with the terms of this SLA. Service Credits expire without refund twelve (12) months from issuance.

Service Credit Request and Application Process

To receive a Service Credit, Customer must submit a claim by logging a support ticket (if Customer is community supported, Customer must email cloud-support@confluent.io). To be eligible, the credit request must be received by Confluent within five (5) calendar days after the last day of the month in which the applicable Cloud Service function does not meet the Service Level, and must include all information reasonably necessary for Confluent to verify the claim, including:

1. the words "SLA Credit Request" in the subject line;
2. a description of the applicable client(s), the version of each such client, and the configurations for each such client; and
3. a description of the events resulting in Downtime, including the time and duration of the Downtime and Customer requests logs that document the failed write attempts.

Confluent will evaluate Customer requests and determine in good faith whether a Service Credit is owed based on its system logs, monitoring reports, configuration records, and other available information. If Confluent confirms that the Monthly Uptime Percentage applicable to the month of such request did not meet the Service Level, then Confluent will issue the Service Credit to Customer within one billing cycle following the month in which Customer's request is confirmed. Customer's failure to provide the request and other information as required above will disqualify Customer from receiving a Service Credit.

Exclusions

This SLA and any applicable Service Level does not apply to any unavailability or performance issues that results from:

1. A suspension described in Section 5.4 of the Agreement (Late Payments) or similar section; Customer's misuse of the Cloud Service in violation of Section 2 of the Agreement (Customer Use) or similar section; or Customer's violation of the Agreement or Confluent's Acceptable Use Policy;
2. Factors outside Confluent's reasonable control, including but not limited to any force majeure event, network intrusions, denial of service attacks, systemic internet issues or any other act or omission of any telecommunication or services provider;
3. Use of services, hardware, or software provided by a third party and not within the primary control of Confluent, including issues resulting from inadequate bandwidth or resulting from failures of cloud platform services on which the Cloud Service runs;
4. Customer's unauthorized action or lack of action when required, including those of Customer's Users or by means of Customer's passwords;
5. Customer's failure to use Confluent-supported Kafka clients with acceptable configuration values as defined in the Cloud Service documentation;
6. Customer-controlled actions and/or environment or other failures or shortcomings not within Confluent's control;
7. Failure by Customer to take any remedial action in relation to the Services as recommended by Confluent, or otherwise preventing Confluent from doing so;
8. Customer's negligence or willful misconduct, including failure to follow agreed-upon procedures;
9. Scheduled maintenance that takes place upon five (5) days email notice or ad hoc maintenance carried out to avoid future unavailability, and/or updates;

10. Customer's failure to provide information required by Confluent to provision the Cloud Service; or
11. Deployment on any Jio region, except as noted in Service Specific Terms below.

Service Specific Terms

Confluent Cloud

Additional Definitions

- **"Downtime"** is the total accumulated minutes during a calendar month for a given Cloud Service cluster during which the entire cluster is unavailable. A minute is considered unavailable for a given cluster if all continuous attempts by Confluent's monitoring system to write to the cluster within the minute fail.
- **"Monthly Uptime Percentage"** means the total number of minutes in a calendar month, minus the number of minutes of Downtime in such month, divided by the total number of minutes in such month. If Customer's Cloud Service cluster is provisioned and running for only part of a calendar month, such cluster is deemed to be 100% available during the portion of the month in which it was not provisioned and running.

<table>
<tr><th colspan="5">Service Credit</th></tr>
<tr><th>Monthly Uptime Percentage</th><th>Basic Cluster</th><th>Standard (1 ECKU) or Enterprise (1 ECKU) Cluster</th><th>Dedicated (Single Zone) Cluster (Including Jio region)</th><th>Standard (2 ECKU), Enterprise (2 ECKU), or Dedicated (Multi-zone) Cluster</th></tr>
<tr><td>< 99.99% ≥ 99%</td><td rowspan="3">-</td><td rowspan="2">-</td><td>-</td><td rowspan="4">10%</td></tr>
<tr><td>< 99.95 ≥ 99%</td><td rowspan="3">10%</td></tr>
<tr><td>< 99.9% ≥ 99%</td><td rowspan="2">10%</td></tr>
<tr><td>< 99.5.% ≥ 99%</td><td>10%</td></tr>
<tr><td>< 99% ≥ 95%</td><td>25%</td><td>25%</td><td>25%</td><td>25%</td></tr>
<tr><td>< 95%</td><td>100%</td><td>100%</td><td>100%</td><td>100%</td></tr>
</table>

Confluent Cloud for Apache Flink®

Additional Definitions

- **"Confluent Cloud for Apache Flink"** means part of the Cloud Service that provides a cloud-native, serverless stream processing service based on Apache Flink, as further described in the Documentation.
- **"Downtime"** is the total accumulated one-minute periods during a calendar month during which

Confluent Cloud for Apache Flink is unavailable in a given cloud region. A one-minute period is considered unavailable for a given region if all continuous requests by Confluent's monitoring system to either the applicable Flink Compute Pool API or Statement API result in a Fail Request.

- **"Fail Request"** means a request that returns an error code or otherwise does not return any successful code within one minute for the GET request due to an issue solely within Confluent's control.
- **"Flink Compute Pool API"** means a software interface used to manage resources used to run Apache Flink workloads, as further described in the Documentation.
- **"Monthly Uptime Percentage"** means the total number of minutes in a calendar month, minus the number of minutes of Downtime in such month, divided by the total number of minutes in such month. If Customer's Confluent Cloud for Apache Flink is provisioned and running for only part of a calendar month, such cluster is deemed to be 100% available during the portion of the month in which it was not provisioned and running.
- **"Statement API"** means a software interface used to model SQL statements for execution in Confluent Cloud for Apache Flink, as further described in the Documentation.

Monthly Uptime Percentage	Service Credit
< 99.99% ≥ 99.9%	5%
< 99.9% ≥ 99.0%	10%
< 99.0%	25%

Confluent Cloud Fully Managed Connectors

Additional Definitions

- "**Confluent Cloud Fully Managed Connectors**" are connectors that are managed and supported by Confluent in the Cloud Service and identified in the Documentation as "Supported". Confluent Cloud Fully Managed Connectors exclude Connect with Confluent connectors, custom connectors, preview connectors, connectors uploaded by Customer to the Cloud Service, or connectors not suitable for production use, as set forth in the Documentation.
- **"Confluent Cloud Fully Managed Connector Instance**" is a deployment of one Confluent Cloud Fully Managed Connector type using one (1) or more Tasks.
- **"Downtime"** is the total accumulated consecutive five-minute periods during a calendar month for a given Confluent Cloud Fully Managed Connector Instance that is unavailable. The consecutive five-minute periods are calculated on a time-based tumbling window. A consecutive five-minute period is considered unavailable for a Confluent Cloud Fully Managed Connector Instance that is in a Failed State for the entire consecutive five-minute period. If a Confluent Cloud Fully Managed Connector Instance has failed due to a User Actionable Error, the Confluent Cloud Fully Managed Connector Instance is considered available.

- **"Failed State"** means the status of a Confluent Cloud Fully Managed Connector Instance where all Tasks for a Confluent Cloud Fully Managed Connector Instance have failed due to an issue solely within Confluent's control.
- **"Monthly Uptime Percentage"** means the total number of consecutive five-minute periods in a calendar month, minus the number of consecutive five-minute periods of Downtime in such month, divided by the total number of consecutive five-minute periods in such month. If Customer's Confluent Cloud Fully Managed Connector Instance is provisioned and running for only part of a calendar month, such instance is deemed to be 100% available during the portion of the month in which it was not provisioned and running.
- **"Task"** means a logical unit of work copying data.
- **"User Actionable Error"** represents a failure in any Task for the Confluent Cloud Fully Managed Connector Instance that is caused by the Customer. User Actionable Error includes an error that causes any Task for the Confluent Cloud Fully Managed Connector Instance to fail due to the Confluent Cloud Fully Managed Connector Instance being configured incorrectly by Customer, connections to external systems, throttling caused by Customer, and Customer server-side issues.

<table>
<tr><th colspan="4">Service Credit</th></tr>
<tr><th>Monthly Uptime Percentage</th><th>Confluent Cloud Fully Managed Connector Instance connecting to a Multi-zone Dedicated, Enterprise, or Standard Cluster</th><th>Confluent Cloud Fully Managed Connector Instance connecting to a Single-zone Dedicated or Standard Cluster</th><th>Confluent Cloud Fully Managed Connector Instance connecting to a Basic Cluster</th></tr>
<tr><td>< 99.99% ≥ 99.95%</td><td rowspan="3">10%</td><td>-</td><td rowspan="2">-</td></tr>
<tr><td>< 99.95% ≥ 99.5%</td><td rowspan="2">10%</td></tr>
<tr><td>< 99.5% ≥ 99%</td><td>10%</td></tr>
<tr><td>< 99%</td><td>25%</td><td>25%</td><td>25%</td></tr>
</table>

Confluent Cloud KSQL

Additional Definitions

- **"Downtime"** is the total accumulated five-minute periods during a calendar month for a given ksqlDB Instance during which the entire ksqlDB Instance is unavailable. A five-minute period is considered unavailable for a given ksqlDB Instance if all Metadata Request attempts within the five-minute period fail.
- **"ksqlDB Instance"** is a multi-zone ksqlDB deployment using eight (8) or more Confluent Streaming Units.

- **"Metadata Request"** is any of the following requests as detailed in the Documentation: LIST STREAMS; LIST TABLES; or LIST QUERIES.
- **"Monthly Uptime Percentage"** means the total number of five-minute periods in a calendar month, minus the number of five-minute periods of Downtime in such month, divided by the total number of five-minute periods in such month. If Customer's ksqlDB Instance is provisioned and running for only part of a calendar month, such instance is deemed to be 100% available during the portion of the month in which it was not provisioned and running.

Monthly Uptime Percentage	Service Credit
< 99.9% ≥ 99.5%	5%
< 99.5% ≥ 99.0%	10%
< 99.0%	25%

Confluent Cloud Schema Registry

Additional Definitions

- **"Downtime"** is the total accumulated minutes during a calendar month for a given Confluent Cloud Service Schema Registry cluster during which the entire cluster is unavailable. A minute is considered unavailable for a given cluster if all continuous attempts by Confluent's monitoring system to write to the cluster within the minute fail.
- **"Monthly Uptime Percentage"** means the total number of minutes in a calendar month, minus the number of minutes of Downtime in such month, divided by the total number of minutes in such month. If Customer's Confluent Cloud Service Schema Registry cluster is provisioned and running for only part of a calendar month, such cluster is deemed to be 100% available during the portion of the month in which it was not provisioned and running.

<table>
<tr><th colspan="4">Service Credit</th></tr>
<tr><th>Monthly Uptime Percentage</th><th>Stream Governance Essentials (Including Jio region)</th><th>Stream Governance Advanced</th><th>Stream Governance Advanced for Jio region</th></tr>
<tr><td>< 99.99% ≥ 99.95%</td><td rowspan="2">-</td><td rowspan="2">5%</td><td>-</td></tr>
<tr><td><99.95% ≥ 99.5%</td><td>5%</td></tr>
</table>

< 99.5% ≥ 99.0%	5%	10%	10%
< 99.0%	10%	25%	25%

Warpstream BYOC

Additional Definitions

- **“Downtime”** is the total accumulated minutes during a calendar month for a given Platform cluster during which the entire Platform cluster is Materially Degraded.
- **"Materially Degraded"** means that all continuous monitoring probe attempts by Confluent's monitoring system fail within a one minute period for a given Platform cluster.
- **“Monthly Uptime Percentage”** means the total number of minutes in a calendar month, minus the number of minutes of Downtime in such month, divided by the total number of minutes in such month. If Customer’s Platform cluster is provisioned and running for only part of a calendar month, such cluster is deemed to be 100% available during the portion of the month in which it was not provisioned and running.

Service Credit				
Monthly Uptime Percentage	**Fundamentals Cluster**	**Pro Cluster**	**Enterprise Cluster (Single Region)**	**Enterprise Cluster (Multi Region)**
< 99.999% ≥ 99.99%	-	-	-	10%
< 99.99% ≥ 99.95%	-	-	10%	10%
< 99.95% ≥ 99.90%	-	10%	10%	10%
< 99.90% ≥ 99.00%	10%	15%	15%	15%
< 99.00% ≥ 95.00%	25%	25%	25%	25%
< 95.00%	100%	100%	100%	100%

CONFLUENT

CONFLUENT CLOUD SUPPORT SERVICES POLICY

Updated October 27, 2025

This document describes Confluent's support policies for customers of the Confluent Cloud Service who have purchased a support services plan in connection with their use of the Cloud Service. It provides a description of the available technical support levels and describes Confluent's terms and conditions for support. Capitalized terms not defined herein have the meaning set forth in the agreement that applies to Customer's use of the Cloud Service.

1. Support Services.

1.1 Confluent offers 3 levels of Support Services plans for Confluent Cloud: Developer, Business, and Premier. This Support Services Policy applies to all levels of Support Services, except to the extent that variations are specifically described herein.

1.2 Customer Support Channels: Confluent shall provide the Support Services through its online support portal ("Support Portal"). Following submission of a Support Request, Confluent will communicate with Customer using email, the Support Portal, or video conferencing. Any necessary telephone support discussions will be scheduled in advance at a time mutually agreed by the parties and for durations and at a frequency that is commercially reasonable for Confluent. Support Services will be provided in English.

1.3 Hours of Operation: Customer may access the Support Portal and submit Support Requests twenty- four (24) hours a day, seven (7) days per week.

1.4 Support Request Prioritization & Confluent Actions: Support Requests will be categorized by priority level in accordance with the following definitions and Confluent will take the following actions:

Support Request Priority Definitions & Confluent Actions

Priority Level	Definition	Confluent Actions
P1	Priority One means that, due to an Issue, the Cloud Service used by Customer in production is severely impacted or completely shut down.	Confluent will: (i) assign specialists to work continuously to correct the Issue; (ii) provide ongoing communication on the status of the Update or Issue resolution; and (iii) simultaneously begin work to provide a temporary workaround or fix.

P2	Priority Two means (i) due to an Issue, the Cloud Service is functioning with limited capabilities, or the Cloud Service is unstable with periodic interruptions, or (ii) there is an Issue in an application in development that is in final testing, facing a critical time frame of going into production use.	Confluent will: (i) assign specialists to correct the Issue; (ii) provide ongoing communication on the status of the Update or Issue resolution; and (iii) simultaneously begin work to provide a temporary Workaround or Fix.
P3	Priority Three means there (i) are Issues with workaround solutions in fully operational Cloud Services, (ii) there are Issues in non-critical functions, or (iii) there is a time sensitive Issue affecting performance or deliverables.	Confluent will use resources during local Business Hours until the Issue is resolved or a Workaround is in place.
P4	Priority Four means there (i) is a need to clarify procedures or information in documentation, (ii) there is a request for a product enhancement or new feature, (iii) cosmetic or non-functional Issues; or (iv) issues in Documentation.	Confluent will triage the request, provide clarification when possible, and may include a resolution in a future Update.

During the submission process, Customer may assign a priority level to a Support Request. Confluent will review Customer's priority designation and respond in accordance with the applicable Target Initial Response Time. However, Confluent may re-assign the priority level if it believes Customer's designation to be incorrect based on the definitions specified in this Support Policy. Confluent will notify Customer of such a change in its response to the Support Request.

1.5 Responses. A "Response" is an initial reply to the Support Request. The "Target First Response Times" shall be measured by the elapsed time between Confluent's receipt of a Support Request and the time when Confluent begins to address it, by responding and initiating communication with Customer about the Support Request. The actual time required to fully resolve an Issue or Support Request, if such full resolution occurs, may be longer than the Target First Response Time. Customer understands and agrees that resolution of an Issue or Request is not guaranteed and may not occur.

Target First Response Times			
Priority Level	**Support Level**		
	Developer	**Business**	**Premier**
P1	Within 8 Business Hours	Within 60 minutes	Within 30 minutes
P2	Within 8 Business Hours	Within 4 hours	Within 2 hours
P3	Within 8 Business Hours	Within 8 Business Hours	Within 8 Business Hours
P4	Within 2 Business Days	Within 2 Business Days	Within 2 Business Days

1.6 Customer Responsibilities: Confluent's obligation to provide Support Services is conditioned upon Customer satisfying the following responsibilities with respect to each Issue:

A) Customer making reasonable efforts to resolve the Issue before reporting the Issue to Confluent, including having the Issue reviewed by the representative of the Customer that submits the Support Request;
B) Customer providing Confluent with sufficient information, including any reproducible test cases requested by Confluent;
C) (For P1 and P2 Requests only) Customer designating personnel resources to provide necessary diagnostic information until a fix or workaround is made available.

2.0. Exclusions. Notwithstanding anything to the contrary in this Support Services policy or the Agreement, Confluent is not obligated to continue work on a Support Request when Confluent determines that:

a. The reported issue has been caused by Customer's negligence, hardware malfunction, network latency or causes beyond the reasonable control of Confluent;
b. The reported issue has been caused by third party software not managed by Confluent as part of the Cloud Service, unless the Documentation requires the software for proper use of the Cloud Service;
c. The reported issue has been caused by Customer's use of the Cloud Service other than in accordance with the configuration and operation guidelines described in the Documentation (e.g., failure to use Confluent-supported Kafka clients with acceptable configuration values).
d. The relevant order for Support Services is expired or no longer in effect.

3.0 Customer Success Technical Architect - Premier Support. If you purchase Premier Support, then during the period for which you purchase such support, Confluent shall provide a customer success technical architect resource ("CSTA") to your account; provided, however, Confluent does not provide a CSTA for the BYOC Service, except as explicitly set forth on an Order. A Confluent CSTA helps customers align Confluent products to business needs, through general product knowledge and proactive engagement. Your CSTA can guide your technical roadmap and facilitate other services across Confluent, including product, support services, and professional services. As needed, your CSTA may engage other experts within Confluent to provide deeper product and use case expertise. Please note that a CSTA's responsibilities are to provide general product knowledge and do not encompass more detailed product expertise or implementation guidance provided through Confluent Professional Services.

The following are representative responsibilities of the CSTA:

- Driving efficient application of purchased Confluent services - e.g. training, professional services and support
- Quarterly technical reviews
- Bi-weekly, remote office hours to discuss topics related to:
  - Project management
  - Development of Confluent Platform-related components
  - Architecture and configuration choices
  - Best practices for Confluent Enterprise monitoring, automation and integrations
  - Upgrade and migration planning
- Keeping your team informed and up to speed on product releases and recommending the

best solutions for your needs
- Facilitates delivery of detailed postmortem reports following production incidents
- Serving as your voice within Confluent, including lobbying for your roadmap priorities

If you purchase both Premier Support for Confluent Cloud and Platinum-level Support Services for Confluent Platform, Confluent will provide a CSTA resource to perform the responsibilities described above, and the meeting frequency described above will be inclusive of both Cloud and Confluent Platform (i.e., the meetings will be consolidated, not duplicated).

4.0 Kafka Streams. As set forth in the Documentation, Confluent will provide Support Services in accordance with the applicable Support Services plan (excluding Basic or Developer) for Customer's deployment of Kafka Streams and subject to payment of additional fees set forth in the Rate Card, provided that Customer utilizes Kafka Streams solely in connection with the Cloud Service. Confluent will not provide Support Services for Kafka Streams when used to support self-managed Kafka brokers.

5.0 Definitions.
- "Business Day" means Monday through Friday in Customer's local time zone.
- "Business Hours" means 9:00 a.m. to 5:00 p.m. on Business Days.
- "Customer Representative" means the individual employee of Customer that submits a Support Request via phone, email or through the Support Portal.
- "Documentation" means the published documentation describing the functionality of the Cloud Service, located at https://docs.confluent.io/current/cloud/index.html#cloud-home.
- "Issue" means a failure of the Cloud Service to conform to the specifications set forth in the Documentation.
- "Support Request" means a support request or Issue submitted by Customer as described in this Support Services Policy.
- "Support Services" means the support services purchased by Customer and described in this Support Services Policy.

6.0 Support Level Election. Support Services for Confluent Cloud are elected and purchased on a self-service basis in the Cloud Service user interface. If Customer elects Premier-level Support Services, then (a) such Support Services must be maintained at the Premier level for the entire term of the applicable Order, and (b) following such Order term, such Premier-level Support Services will end, unless Customer enters into a new commitment Order. If Customer elects Business-level Support Services and also has an Order for Confluent Platform then the Confluent Cloud Support Services must be maintained at the Business level for the entire term of the applicable Order.

7.0 Changes to Support Services Policy. This Support Services Policy may be updated from time to time at Confluent's sole discretion, provided that any such updates will not materially reduce the level of Support Services during the period for which Customer has purchased Support Services. Any material changes to this Support Services Policy will not apply unless and until such changed terms are accepted by the Customer.

ACCEPTABLE USE POLICY

This Confluent acceptable use policy ("AUP") sets forth certain restrictions relating to use of the Cloud Service or any other Confluent products by Customer or Users under Customer's agreement with Confluent ("Agreement"). Any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement.

Customer agrees not to (and shall not permit its Users or other third parties to) use the Cloud Service or any other Confluent products:

1. to transmit, store, or make available (a) Content that is illegal, threatening, fraudulent, or in violation of any third party rights, including privacy or intellectual property rights; or (b) viruses, malware, or other malicious code;

2. for illegal, threatening, disruptive, or offensive uses;

3. to make it available to anyone other than its Users as explicitly set forth in the Agreement;

4. to violate the security or integrity of any network, computer or communications system, software application, or network or computing device, including to attempt to or to perform account takeovers by brute-force attacks or other means;

5. to distribute unsolicited emails or other communications, including using an unauthorized email account;

6. to make network connections to any users, hosts, or networks unless Customer has permission to communicate with them, including to perform any denial of service or distributed denial of service attacks;

7. to use manual or electronic means to avoid any use limitations placed on the Cloud Service (such as access and storage restrictions) or to bypass any paywalls or otherwise use features beyond what is allowed by the free tiers;

8. to transmit Protected Health Information (as defined under HIPAA) into the Cloud Service without first having entered into a BAA with Confluent;

9. to transmit cardholder or sensitive authentication data (as those terms are defined in the PCI DSS standards) ("PCI Data") unless the PCI Data is message-level encrypted by Customer and Customer uses only private networking for Cloud Service clusters;

10. to perform any security penetration tests or security assessment activities without the express, prior written consent of Confluent's Chief Information Security Officer; or

11. to perform any benchmarking against any products or services competitive to Confluent or any other competitive purpose.

Notwithstanding anything to the contrary in the Agreement, in the event of any conflict between the Agreement and this AUP, this AUP shall govern. Confluent may change this AUP from time to time and such changes will be effective when posted. Any material changes to this AUP will not apply unless and until such changed terms are accepted by the Customer. Confluent may temporarily remove or suspend any particular Customer content for any violation of this AUP that poses immediate risk to the security or functionality of the Cloud Service, or that risks violation of applicable law or legal rights of Confluent or third parties.

Confluent Data Processing Addendum

Updated: October 12, 2025

This Data Processing Addendum ("**DPA**") forms part of the Confluent Cloud Services Agreement or other applicable written or electronic terms of service or subscription agreement ("**Agreement**") between the Confluent entity which entered into the Agreement ("**Confluent**") and the **Customer** signatory thereto. All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement. The parties agree that this DPA shall replace any existing DPA or other data protection provisions the parties may have previously entered into in connection with the Services.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. Scope and Term of the DPA.

1.1. Scope. This DPA applies to the extent Confluent processes Personal Data in the course of providing Services to the Customer pursuant to the Agreement, as further described in this DPA and its Schedules.

1.2. Term. The term of this DPA coincides with the term of the Agreement and terminates upon expiration or earlier termination of the Agreement (or, if later, the date on which Confluent ceases all Processing of Customer Personal Data).

2. Roles and Details of Processing.

2.1. Role of the Parties.

2.1.1. Customer may act as Controller and/or Processor of Customer Personal Data. Confluent may act as Processor and/or Subprocessor of Customer Personal Data.

2.1.2. Confluent acts as a Controller of Account Data.

Details regarding the processing of Personal Data are provided in **Schedule 1** (Details of Processing).

2.2. Customer as Controller of Customer Personal Data. If Customer is Controller of Customer Personal Data, Customer agrees that (i) it will comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Customer Personal Data and any processing instructions it issues to Confluent; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary for Confluent to process Customer Personal Data pursuant to the Agreement and this DPA.

2.3. Customer as Processor of Customer Personal Data. If Customer is Processor of Customer Personal Data, Customer warrants on an ongoing basis that the relevant Controller has authorized: (i) Confluent's processing of Customer Personal Data as outlined in this DPA, including its Schedules; (ii) Customer's appointment of Confluent as another processor; and (iii) Confluent's engagement of Subprocessors as described in Section 3 (Subprocessing) below.

2.4. Customer Instructions. Confluent will process Customer Personal Data solely in accordance with Customer's documented lawful instructions as set forth in the Agreement and this DPA to (i) provide the Services, and enable the use of various features and functionalities in accordance with the Documentation (including as directed by Users through the use of Services); (ii) investigate and resolve issues, bugs and errors (troubleshooting), including Security Incidents; or (iii) as permitted by law. Confluent shall inform Customer if, in its opinion, Customer's processing instruction infringes applicable Data Protection Laws. The parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the processing are set out in this DPA. Confluent certifies that it understands the restrictions in this Section 2.4 (Customer Instructions) and will comply with such restrictions.

3. Subprocessing.

3.1. Authorized Subprocessors. Customer agrees that in order to provide the Services, Confluent may engage Subprocessors to process Customer Personal Data. Confluent maintains a list of its authorized Subprocessors on its website at https://www.confluent.io/sub-processors/. Customer will receive

notifications of new Subprocessors and updates to existing Subprocessors by subscribing for updates at https://www.confluent.io/subscribe-to-sub-processor-updates.

3.2. Subprocessor Obligations. Where Confluent authorizes any Subprocessor as described in Section 3.1 (Authorized Subprocessors) above:

3.2.1. Access to Customer Personal Data will be limited only to what is necessary to assist Confluent in providing or maintaining the Services, and Subprocessor will be prohibited from accessing Customer Personal Data for any other purpose;

3.2.2. Confluent will enter or has already entered into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor to protect the Customer Personal Data to the standard required by applicable Data Protection Laws; and

3.2.3. Confluent will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause Confluent to breach any of its obligations under this DPA.

Upon request and subject to any pre-existing confidentiality obligations, Confluent will provide Customer with all the relevant information it reasonably can in connection with its applicable Subprocessor agreements when required to satisfy Customer's obligations under applicable Data Protection Laws.

3.3. Subprocessor Updates. Confluent will provide Customer with a 30-day prior notice on its website if it intends to make any changes to its Subprocessors ("**Notice Period**"). Customer may object in writing to Confluent's appointment of a new Subprocessor during the Notice Period, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties will discuss the objection in good faith with a view to achieving resolution, allowing for an additional 30-day period for such discussions ("**Grace Period**"). For the avoidance of doubt, the intended change of the Subprocessor will not be affected by the Grace Period. If during the Grace Period the parties are not able to achieve a satisfactory resolution, Customer, as its sole and exclusive remedy, may terminate the applicable Order for the relevant Service within ten (10) days after the end of the Grace Period (without prejudice to any paid or outstanding fees incurred or committed by Customer prior to termination).

4. Security Measures and Security Incident Response

4.1. Security Measures. Confluent has implemented and will maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data ("**Security Measures**"). The Security Measures applicable to the Cloud Service are set forth in the Confluent Cloud Security Addendum available at https://www.confluent.io/cloud-enterprise-security-addendum and in the and in the Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data ("TOMS") available at https://assets.confluent.io/m/58d577a09eda0716/original/TOMs-Modules-Two-and-Three-LEGAL.pdf, as updated or replaced from time to time in accordance with Section 4.2 (Updates to Security Measures) below.

4.2. Updates to Security Measures. Customer has carried out its own review of the information made available by Confluent relating to data security and has made an independent determination that the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Confluent may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of Cloud Service purchased by the Customer.

4.3. Security Incident. In the event of a Security Incident, Confluent will notify Customer without undue delay, and in any case, where feasible, within seventy-two (72) hours of a confirmed Security Incident

and will provide updates to Customer. Confluent will reasonably cooperate with Customer as required to fulfil Customer's obligations under Data Protection Laws.

4.4. Confidentiality. Confluent restricts its personnel from processing Customer Personal Data without authorization by Confluent as set forth in the Security Measures and shall ensure that any person who is authorized by Confluent to process Customer Personal Data is under an appropriate obligation of confidentiality and agrees to comply with applicable Data Protection Laws.

4.5. Customer Responsibilities. Without prejudice to Confluent's obligations under this DPA, and elsewhere in the Agreement, Customer is responsible for its secure use of the Services, including: (i) protecting account authentication credentials; (ii) protecting the security of Customer Personal Data when in transit to and from the Services; (iii) implementing measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (iv) taking any appropriate steps to securely encrypt or pseudonymise any Customer Personal Data uploaded to the Services.

5. Audits.

To the extent Customer's audit requirements under applicable Data Protection Laws cannot reasonably be satisfied through Confluent's relevant audit reports and certifications ("**Audit Reports**"), documentation or compliance information Confluent makes generally available to its customers or through reasonably written audit questions, which Customer may request no more than once per calendar year, Confluent will promptly respond to Customer's additional audit requests. Before the commencement of an audit, Customer and Confluent will mutually agree upon the scope, timing, duration, and control and evidence requirements, provided that this requirement to agree will not permit Confluent to unreasonably delay performance of the audit. To the extent needed to perform the audit, Confluent will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Personal Data by Confluent available. Neither Customer nor the third-party auditors, if any, shall have access to any data from Confluent's other customers or to Confluent systems or facilities not involved in the processing of Customer Personal Data. Customer is responsible for all costs and expenses related to such audit, including all reasonable costs and expenses for any and all time Confluent expends for any such audit.

6. Return or Deletion of Customer Personal Data.

Upon termination or expiration of the Agreement, Confluent shall (at Customer's election) delete or return (in the same format sent to Confluent) all Customer Personal Data in its possession or control in accordance with the terms of the Agreement.

7. Cooperation.

7.1. Data Subject Request. The Services provide Customer with the ability to retrieve and delete Customer Personal Data. Customer may use these controls to comply with Customer's obligations under applicable Data Protection Laws, including Customer's obligations related to any requests from data subjects involving Customer Personal Data ("**Data Subject Requests**"). To the extent that Customer is unable to independently access the relevant Customer Personal Data using such controls or otherwise, Confluent shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to such Data Subject Requests. In the event that any such Data Subject Request is made directly to Confluent, Confluent shall, to the extent legally permitted: (i) advise the data subject to submit their Data Subject Request to Customer; (ii) promptly notify Customer; and (iii) not otherwise respond to that Data Subject Request without authorization from Customer unless legally compelled to do so. Customer will be responsible for responding to any such Data Subject Requests.

7.2. Requests for Customer Personal Data. If Confluent receives a subpoena, court order, warrant or other legal demand from law enforcement or public or judicial authorities seeking the disclosure of Customer Personal Data, Confluent shall, to the extent permitted by applicable laws, promptly notify Customer in

writing of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

7.3. Legal Compliance. To the extent Confluent is required under applicable Data Protection Laws, Confluent will (at Customer's expense) provide reasonably requested information regarding the Cloud Service to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities, taking into account the nature of processing and the information available to Confluent.

8. Final Provisions.

8.1. For the avoidance of doubt, any claim or remedies the Customer and/or its Affiliates may have against Confluent, any of its Affiliates and their respective employees, agents and Subprocessors (hereinafter "**Confluent Group**") arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) for breach of cross-border data transfers and related provisions outlined in the Standard Contractual Clauses (to the extent applicable and as defined in **Schedule 2** hereto); (iii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; and (iv) under applicable Data Protection Laws, including any claims relating to damages paid to a data subject, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Such limitation of liability does not apply to any direct claim or remedies a data subject may have against Customer or Confluent. Customer further agrees that any regulatory penalties incurred by Confluent Group in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Confluent's liability under the Agreement as if it were liability to the Customer under the Agreement.

8.2. Any claims against Confluent or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

8.3. To the extent reasonably necessary to comply with changes to applicable Data Protection Laws or in response to guidance or mandates issued by any court, regulatory body, or supervisory authority with jurisdiction over Confluent, Confluent may modify, amend, or supplement the terms of this DPA. Confluent will endeavour to provide prior written notice of any such changes to Customer by posting a notice on Confluent's website and/or in Customer's Confluent Cloud web portal, where applicable.

8.4. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

8.5. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in **Schedule 2** (Jurisdiction-Specific Terms); (2) the terms of this DPA; and (3) the Agreement. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

8.6. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA, and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

9. Definitions.

9.1. "**Account Data**" means Personal Data relating to Customer's relationship with Confluent, including: (i) Users' account information (e.g. name, email, User ID); (ii) billing and business contact information of individual(s) associated with Customer's account (e.g. billing address, email, name); (iii) Users' device, browser, and connection information (e.g. IP address); and (iv) Personal Data provided during Support requests. For the avoidance of doubt, Account Data does not include Customer Personal Data.

9.2. "**Customer Personal Data**" means any Personal Data uploaded by Customer or its Users into the Cloud Service that Confluent processes solely on behalf of Customer in the course of providing the Services. Customer acknowledges that it solely determines the nature and types of Customer Personal Data.

9.3. "**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

9.4. "**Security Incident**" means an unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

9.5. "**Services**" means any cloud service offering provided by Confluent to Customer pursuant to the Agreement.

9.6. "**Subprocessor**" means any Processor engaged by Confluent or its Affiliates to process Customer Personal Data. Subprocessors may include third parties or Confluent's Affiliates.

9.7. The terms "**Business**", "**collect**", "**Consumer**", "**Controller**", "**Data Subject**", "**Processor**," "**process**,", "**processing**", "**Personal Data**", and "**Service Provider**" have the meanings given to them in applicable Data Protection Laws.

Schedule 1
Details of Processing

1. **Categories of data subjects whose Personal Data is Processed:** Customer, Customer's Users, employees, contractors, suppliers, and other third parties as determined solely by the Customer.
2. **Categories of Personal Data Processed:** Customer Personal Data; Account Data.
3. **Sensitive data transferred**.

3.1. Customer Personal Data: Customer may submit special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences) to the Cloud Service, the extent of which is determined and controlled by Customer in its sole discretion. Customer is responsible for ensuring a level of data protection commensurate with the sensitivity of the Customer Personal Data including, without limitation, an appropriate level of message-level encryption, according to the terms of the Confluent Cloud Security Addendum.

3.2. Account Data: None.

4. **The frequency of the transfer**: Continuous.
5. **Nature of the Processing**: Confluent will Process Personal Data to provide the Cloud Service and Support Services in accordance with the Agreement, including this DPA. Additional information regarding the nature of the Processing (including transfer) is described in respective Orders and Documentation referring to technical capabilities and features, including but not limited to collection, structuring, storage, transmission, or otherwise making available of Personal Data by automated means.
6. **Purpose(s) of the Processing.**

6.1. Customer Personal Data: Confluent will process Customer Personal Data in accordance with Section 2.4 (Customer Instructions) of the DPA.

6.2. Account Data: Confluent will process Account Data for Confluent's legitimate business purposes, including to:

- 6.2.1. manage the relationship with the Customer, as well as the communication, billing and overall administration of the Customer account(s).
- 6.2.2. provide, maintain, and improve Cloud Service and Support Services.
- 6.2.3. enhance the overall security of Cloud Service, including but not limited to investigating Security Incidents, fraud monitoring and prevention, business continuity and disaster recovery.
- 6.2.4. Provide Users with product, marketing and other communications in accordance with their preferences.
- 6.2.5. Comply with its legal obligations.

Confluent's processing of Account Data shall comply with applicable Data Protection Laws. Confluent's Controller activities are described in its Privacy Notice available at https://www.confluent.io/legal/confluent-privacy-statement.

7. **Duration of Processing.**

7.1. Customer Personal Data: Confluent will Process Customer Personal Data for the term of the Agreement as outlined in Section 6 (Deletion and Return of Customer Personal Data).

7.2. Account Data: Confluent will Process Account Data only as long as required (a) to provide the Services to Customer in accordance with the Agreement; (b) for Confluent's legitimate business purposes outlined in Section 6.2 of this **Schedule 1**, in which case such retention period shall comply with applicable Data Protection Laws; or (c) by applicable Law(s).

8. **Transfers to Subprocessors**: Confluent will transfer Customer Personal Data to Subprocessors as permitted in Section 3 (Subprocessing).

CONFLUENT

Schedule 2

Jurisdiction-Specific Terms

Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this Schedule will have the meanings given to them in Section 3 (Definitions) of this Schedule.

1. Europe, Switzerland and United Kingdom.

1.1. Data Privacy Framework. Confluent participates in and self-certifies compliance with the Data Privacy Framework ("**DPF**") to implement appropriate safeguards for transfers of Personal Data to the United States pursuant to Art. 46 of the GDPR. To the extent the DPF can be used to lawfully transfer Customer Personal Data to the United States, and for as long as Confluent is self-certified to the DPF, Confluent will adhere to the DPF Principles, including by: (a) processing Customer Personal Data only for the limited and specified purposes set out in the Agreement, including this DPA; (b) providing at least the same level of privacy protection to the Customer Personal Data as is required by the DPF Principles; (c) promptly notifying the Customer if it makes a determination that it can no longer meet its obligation under (b) above, and (d) will, upon written notice, take reasonable and appropriate steps to remediate any unauthorized processing of Personal Data.

1.2. European Data Transfers. In addition to the DPF, where Personal Data protected by the GDPR is transferred, either directly or via onward transfer, to a country outside of Europe that is not subject to an adequacy decision the parties rely on the following transfer mechanisms:

1.2.1. The EU SCCs are hereby incorporated into this DPA by reference as follows:

i. Customer is the "data exporter" and Confluent is the "data importer".

ii. Module One (Controller to Controller) applies where Confluent is Processing Account Data.

iii. Module Two (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Confluent is Processing Customer Personal data as a Processor.

iv. Module Three (Processor to Processor) applies where Customer is a Processor of Customer Personal Data and Confluent is processing Customer Personal Data as another Processor.

v. By entering into this DPA, each party is deemed to have signed the EU SCCs as of the commencement date of the Agreement.

1.2.2. For each Module, where applicable:

i. In Clause 7, the optional docking clause shall apply.

ii. In Clause 9, Option 2 applies, and the time period for prior notice of Subprocessor changes is stated in Section 3 (Subprocessing) of this DPA.

iii. In Clause 11, the optional language does not apply.

iv. In Clause 17, Option 1 applies, and the EU SCCs are governed by German law.

v. In Clause 18(b), disputes will be resolved before the courts of Munich.

vi. The Appendix of EU SCCs is populated as follows:

- The information required for Annex I(A) is in the Agreement and/or relevant Orders.
- The information required for Annex I(B) is in **Schedule 1** (Description of Processing) of this DPA.
- The competent supervisory authority in Annex I(C) will be determined in accordance with the applicable Data Protection Law; and
- The information required for Annex II is located (a) for Module One at https://assets.confluent.io/m/3233a9f4ddf8fb64/original/Annex-II-TOMs-Module-One-LEGAL.pdf, and (b) for Modules Two and Three at https://www.confluent.io/cloud-enterprise-security-addendum.

1.3. Swiss Transfers. In addition to the DPF, where Personal Data protected by the Swiss FADP is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in Section 1.2 (European Transfers) above with the following modifications:

1.3.1. All references in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP; all references to the General Data Protection Act in this DPA will be interpreted as references to the FADP.

1.3.2. In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

1.3.3. In Clause 17, the EU SCCs are governed by the laws of Switzerland.

1.3.4. In Clause 18(b), disputes will be resolved before the courts of Switzerland.

1.3.5. All references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

1.4. United Kingdom Transfers. In addition to the DPF, where Personal Data protected by the UK GDPR is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:

1.4.1. The EU SCCs apply as set forth in Section 1.2 (European Transfers) above with the following modifications:

i. Each party shall be deemed to have signed the UK Addendum.

ii. For Table 1 of the UK Addendum, the parties' key contact information is located in the Agreement and/or relevant Orders.

iii. For Table 2 of the UK Addendum, the relevant information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to is located above in Section 1.2 (European Transfers) of this Schedule.

iv. For Table 3 of the UK Addendum:

- The information required for Annex 1A is in the Agreement and/or relevant Orders.
- The Information required for Annex 1B is in **Schedule 1** (Description of Processing) of this DPA.
- The information required for Annex II is located (a) for Module One at https://assets.confluent.io/m/3233a9f4ddf8fb64/original/Annex-II-TOMs-Module-One-LEGAL.pdf, and (b) for Modules Two and Three at https://www.confluent.io/cloud-enterprise-security-addendum.
- The information required for Annex III is located in Section 3 (Subprocessing) of this DPA.

1.4.2. In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

1.5. Confluent Europe Limited as a Party to the Agreement. If Confluent Europe Limited is a party to the Agreement and, respectively, this DPA, the provisions of Sections 1.1, 1.2, 1.3 and 1.4. above regarding the relevant transfer mechanisms shall not be applicable. This DPA constitutes the documented instruction from the Customer for any onward transfers of Personal Data to third countries by Confluent Europe Limited on the condition that relevant applicable Data Protection Law requirements regarding such onward transfers are met, including for transfers of Customer Personal Data to any Subprocessors in accordance with Section 3 of this DPA.

2. The United States.

2.1. CCPA Compliance. This Section 2 applies to the extent Customer is a Business that is subject to the CCPA and submits Personal Information (as that term is defined under CCPA) as part of Customer Personal Data in connection with Confluent's performance of the Agreement. Customer appoints Confluent as its Service Provider to collect and process the Customer Personal Data for the purposes outlined in Section 2.4 (Customer Instructions) of the DPA. Confluent will not (a) Sell Customer Personal Data; (b) retain, use, or disclose the Customer Personal Data for any purpose other than for the Business Purpose, including to retain, use, or disclose the Customer Personal Data for a commercial purpose other than providing its

Cloud Service or Support Services under the Agreement; (c) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between Confluent and the Customer; (d) process the Customer Personal Data for targeted and/or cross context behavioural advertising; (e) combine Customer Personal Data that it receives from, or on behalf of, Customer, with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the Consumer, if and to the extent such combination would be inconsistent with the limitations on Service Providers under the CCPA or other laws.

3. Definitions.

3.1. Where Personal Data is subject to the laws of one the following regions, the definition of applicable Data Protection Law includes:

3.1.1. **Australia**: The Australian Privacy Act.

3.1.2. **Brazil**: The Brazilian law No. 13,709 of August 14th, 2018, Lei Geral de Proteção de Dados (General Personal Data Protection Act), or "**LGPD**".

3.1.3. **Europe**: The Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, or **GDPR**).

3.1.4. **Switzerland**: The Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time ("**Swiss FADP**").

3.1.5. **The United Kingdom**: The Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 as amended, superseded or replaced from time to time ("**UK GDPR**").

3.1.6. **The United States**: All state laws relating to the protection and processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations ("**CCPA**"), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act ("**US State Privacy Laws**").

3.2. "**Data Privacy Framework**" or "**DPF**" means, as applicable, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework self-certification program operated by the US Department of Commerce, and their respective successors.

3.3. "**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as amended, superseded or replaced.

3.4. "**Europe**" means, for the purposes of this DPA, the Member States of the European Union and European Economic Area.

3.5. "**EU SCCs**" mean the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, superseded, or replaced from time to time.

3.6. "**Sell**" or "**Sale**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing or by electronic or other means, Customer Personal Data to a third party for monetary or valuable consideration.

3.7. "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.