End User Terms of Service for Pindrop® Cloud Solutions

These End User Terms of Service for Pindrop® Cloud Solutions ("**TOS**") apply to any Products or Services that Pindrop Security, Inc. ("**Pindrop**") provides to your company ("**you**" or "**your**") via an Authorized Reseller. By entering into a Reseller Order, you agree to be bound by this TOS. If you do not agree to the terms of this TOS, you do not have the right to use any Pindrop Property. Pindrop agrees to be bound by this TOS upon acceptance of an order it enters into with the Authorized Reseller relevant to your Reseller Order. Capitalized terms have the meanings given in this TOS.

1. Definitions.

(a) "**Authorized Geography**" means the United States only. For clarity, because you are authorized to access and use the Product in the United States only, then Your Phone Numbers are limited to those intended for use by your United States-based customers to conduct business with your United States-based business operations.

(b) "**Authorized Reseller**" means an entity that is authorized by Pindrop to resell the Products and Services to end user customers.

(c) "**Call**" means a phone call made to Your Phone Number that is processed by a Product.

(d) "**Call Heuristics**" means the duration that a device's touch keys are held down (e.g., the frequency of a caller pressing a device's touch keys).

(e) "**Call Processing Data**" means data (excluding CPNI) obtained by or from a telecommunications network about a Call that is generally used for call routing purposes. Examples of Call Processing Data include data used to initiate, route, exchange, and complete call traffic that is internal to the network.

(f) "**Confirmed Fraud Call**" means a Call You designate through the user interface of the Pindrop® Protect Product (or any subsequent Product having the same functionality) as being associated with fraudulent or suspicious activity.

(g) "**Consortium Members**" means Pindrop customers, government agencies, third party data providers, consumer agencies, credit lenders and other third parties that have themselves provided "fraudulent call data" to Pindrop or its affiliates.

(h) "**CPNI**" or "**Customer Proprietary Network Information**" means data obtained by or from a telecommunications network about a Call that relates to the quality, technical configuration, type, destination, location, or amount of use of the voice service for calls placed from a particular phone number, or is the type of call-related data that would customarily appear on the customer's bill who is purchasing the relevant telecommunications and interconnected VoIP services from a carrier partner. Examples of CPNI include the phone number of the calling party or called party, type of service the customer has ordered or the location of the customer or device.

(i) "**Digital Signal**" means the digital signal used to transmit audio from the device and/or the telecommunications network.

(j) "**Documentation**" means any documentation, user guides and installation instructions Pindrop provides to you from time to time.

(k) "**DTMF**" means the audio sound of the dual tone multiple frequency (i.e., the signal sent when a caller presses a device's touch keys).

(l) "**Effective Date**" means the date on which you first enter into a Reseller Order for Products or Services.

(m) "**Feedback**" means all ideas, suggestions, or similar information that you provide or otherwise make available to Pindrop or its affiliates about Products, Work Product, or Services or any other Pindrop product or service offering.

(n) "**Fraudulent Call Data**" means the following data for a Confirmed Fraud Call: (i) a phone number; (ii) the timestamp, duration, type of number and geography metadata; (iii) call type (e.g., mobile or VOIP); (iv) the Pindrop Score (i.e., the numerical risk score assigned to the Call); and (v) system labels.

(o) "**Laws**" means all laws, statutes, regulations and other types of government authority, including without limitation, the laws and regulations governing data privacy or data protection.

(p) "**Outputs**" means the data or information portion of a Product that are generated using Pindrop's proprietary technology and relevant to a Product's analysis of a Call (including, for example, Pindrop Scores, system labels, Proprietary Prints, or an audio recording of a Call).

(q) "**Pindrop Database**" means Pindrop's proprietary database that includes the Fraudulent Call Data as well as the same or similar data with respect to calls associated with fraudulent or suspicious activity provided by Consortium Members and other information derived from third party data providers and Pindrop's (or its affiliates') own research efforts.

(r) "**Pindrop Property**" has the meaning assigned in Section 6(f) (Pindrop Property) of this TOS.

(s) "**Pindrop Score**" means the scoring metrics, data or reasons for a scoring metric provided by Pindrop's proprietary processes, including statistical and audio models (e.g., phoneprints), intended to predict the likelihood of a phone transaction being fraudulent or suspicious or from someone other than an authenticated caller, as applicable depending on the features and functionality of a given Product.

(t) **"Pre-GA Offering"** means a product or potential new feature or functionality for a Product to which you have an existing subscription that is provided in a Pindrop-managed lab environment and identified as "beta," "limited availability," "pre-release" or similar designation, or that is otherwise identified by Pindrop as unsupported.

(u) "**Product**" means a Pindrop product you order under a Reseller Order, including any Pre-GA Offerings.

(v) "**Professional Services**" or "**PS**" means any implementation services (which may include installation, configuration, project management, process reviews and associated policy or procedure development, testing or go-live support), training, consultancy, or other optional services Pindrop provides as an Authorized Reseller's subcontractor under a Reseller Order.

(w) "**Proprietary Prints**" means the numerical values generated by the Product that are a sequence of floating-point numbers, are not reversible into the original audio, are not composed of an audio wave file, and do not contain any actual recorded conversation. Examples of proprietary prints include: (i) Fakeprints (generic artifacts extracted to detect synthetic or recorded audio - not to identify a person); (ii) Toneprints (unique to device type and carrier – not person); (iii) Phoneprints (unique to device type, carrier and country location – not person; (iv) behavior heuristics (e.g., keypress patterns on device such as to help detect human vs robotic characteristics); and (v) voice features.

(x) "**Reseller Order**" means a document entered into between you and the Authorized Reseller under Your Agreement that describes the Products and Services that will be provided to you subject to this TOS.

(y) "**Services**" means PS or Support Services provided to you under a Reseller Order.

(z) "**Subscription Term**" means the duration that you have the right to access and use a Product.

(aa) "**Support Services**" means the support and maintenance services Pindrop provides to the Authorized Reseller in connection with a given Product.

(bb) "**Support Tools**" means software, web analytics tools or other technology used by Pindrop or its affiliates to (i) monitor, maintain, or improve Product performance, integrity or security, (ii) identify Product errors and maintenance issues, (iii) understand user behavior with a given Product (e.g., what feature or functionality is preferred), which may include the recording of a user's session while logged in to the Product, (iv) manage subscription-related metrics (e.g., quantity of Calls or expiration of a given Subscription Term), or (v) set cookies on a user's browser for the purpose of identifying users and your systems interacting with the Product or to log a user out after a period of inactivity, including the general location (e.g., city, state or country) of the IP addresses associated with users who login into and use a Product.

(cc) "**Telco Network Call Data**" means, collectively, CPNI and Call Processing Data.

(dd) "**User**" means an individual you authorize to use a Product and whom you assign (or, when applicable, Pindrop at your request) a user identification number and password to access the Product.

(ee) "**Work Product**" means any inventions, discoveries, software or other works of authorship (including, without limitation, Product configuration, accuracy reports, and other documentation), and other proprietary materials or work product developed by or for Pindrop or its affiliates, alone or with others, in the course of Pindrop's performance of Services, including any and all related and underlying software, databases (including data models, structures, and data non-specific to you), specifications, technology reports and documentation.

(ff) "**Your Agreement**" means the written agreement between you and the Authorized Reseller under which the Authorized Reseller will make Products and Services available to you.

(gg) "**Your Call Center Infrastructure**" means the telephony solution with which you will use a Product, as contemplated in the Reseller Order.

(hh) "**Your Call Data**" means data and information you upload, transmit, input, or otherwise provide or make available to Pindrop in connection with a Product. Caller phone number, audio (i.e., spoken content), signaling and call-related metadata from your telecommunications network (including the Telco Network Call Data) and Digital Signal for a given Call are examples of Your Call Data.

(ii) "**Your Phone Number**" means a phone number you designate for Product analysis of incoming Calls.

2. Engagement Model. As between Pindrop and Authorized Reseller, Authorized Reseller is solely and exclusively liable for all obligations to you in Your Agreement and under each Reseller Order. Except as expressly provided otherwise in this TOS, you will look solely to Authorized Reseller with respect to your rights and obligations in connection with the Products and Services (including support services and payment of fees), as detailed in Your Agreement and the relevant Reseller Order. Pindrop is not responsible for providing support services directly to you.

3. General Pindrop Responsibilities.

(a) **Provision of Products and Services.** Pindrop will make Products and Services available to you subject to the terms of this TOS, and solely for lawful purposes and use.

(b) **Protection of Your Call Data.** During the Term and for as long as Pindrop maintains your Confidential Information within the Pindrop-Controlled Information Systems (as defined in Exhibit C (Pindrop Information Security and BCP Programs)), Pindrop will have and maintain the information security program and safeguards as detailed Exhibit C (Pindrop Information Security and BCP Programs).

(c) **BCP Program.** Pindrop will maintain and administer a Business Continuity Program ("**BCP**") for the Products, as detailed in Exhibit C (Pindrop Information Security and BCP Programs).

4. Use of Products and Services.

(a) Subscriptions. Unless otherwise provided in the Reseller Order, the Products and Services are purchased as subscriptions for the Subscription Term stated in the Reseller Order.

(b) Access to Products and Services. You have the right to access and use the relevant Products and Services subject to the terms of the Reseller Order, this TOS and the Documentation. The Product may contain Third-Party Software Components (defined below). Your right to use Third-Party Software Components is subject to the relevant third-party terms identified within the Product or the Product's associated Documentation applicable to each Third-Party Software Component. For purposes of this Section, "**Third-Party Software Components**" means third-party software bundled with or included the Product for which Pindrop has an obligation to pass-through open source or proprietary commercial software license terms directly to you from a third-party licensor.

(c) **Your General Responsibilities.** You will (i) be responsible for your Users' compliance with this TOS, the applicable Documentation and Reseller Orders, (ii) be responsible for the accuracy, quality and legality of Your Call Data, including as detailed in Section 7 (Your Warranties) of this TOS, (iii) use commercially reasonable efforts to prevent unauthorized access to and use of Products and Services, and notify Pindrop promptly of any unauthorized access or use, (iv) use Products (including the Outputs) solely to perform phone number fraud verification and/or authentication for your own products or services based on the features and functionality enabled in a given Product and for no other purpose (e.g., not for credit decisioning purposes or to determine a consumer's eligibility for credit or insurance, or for any other permissible purpose set forth in the FCRA (as defined below)), and (v) except as expressly provided otherwise in this TOS, be solely responsible for, and agree to comply with, all applicable Laws with respect to your access and use of the Products and Services. For clarity, Pindrop is not a consumer reporting agency and none of the information provided through the Products constitutes a "consumer report", as the term is defined in the Fair Credit Reporting Act ("**FCRA**"), 15 U.S.C. § 1681 et seq.

(d) **Restrictions.** You will not: (i) make any Pindrop Property available to anyone other than you or your Users, or use any Pindrop Property for the benefit of anyone other than you or your affiliates (unless expressly stated otherwise in this TOS or a Reseller Order), (ii) sell, resell, sublicense, distribute, rent or lease the Pindrop Property in any manner (including without limitation in any service bureau or outsource offering); (iii) copy, modify or create derivative works of all

or any portion of the Pindrop Property; (iv) except to the extent permitted by applicable Law, disassemble, reverse engineer or decompile all or any portion of the Pindrop Property in any manner; (v) frame or mirror any part of the Products, other than framing on your own intranets or otherwise for your own internal business purposes of as permitted in the Documentation; (vi) manually enter and/or import any Your Call Data into a Product that would or could violate Payment Card Industry Data Security Standard (PCI DSS), as amended from time to time, including by way of example only, a credit security validation (CSV) number and a credit card account number (the "**PCI Restriction**"); (vii) attempt to gain unauthorized access to the Products or related systems or networks, or permit direct or indirect access to or use of the Pindrop Property in a way that circumvents contractual usage or security restrictions; (viii) access or use the Pindrop Property to (A) build a competitive product or service, (B) build a product or service using similar ideas, features, functions or graphics of the Pindrop Property, or (C) copy any ideas, features, functions or graphics of the Pindrop Property; or (ix) directly or indirectly authorize any third parties to do any of the foregoing. Any use of the Products in violation of this TOS or the applicable Reseller Order or that in Pindrop's commercially reasonable business judgment threatens the security, integrity or availability of the Product to Pindrop's customers, may result in immediate suspension of your access to the Product. However, Pindrop will use commercially reasonable efforts under the circumstances to provide you with written notice (email is sufficient) and an opportunity to remedy the violation or threat prior to suspension. Further, if a breach occurs with respect to the Outputs, Pindrop reserves the right to require you to delete and/or destroy the Outputs (as well as any derivative works, benchmarking or competing solution) in your possession or control.

(e) **Special Terms for Pre-Ga Offerings.** Pindrop may make Pre-GA Offerings available to you from time to time. Pre-GA Offerings are subject to the same terms in this TOS, except as provided otherwise in this Section or a Reseller Order. Pre-GA Offerings are provided on an "as is" basis and are not included in Pindrop's support obligations to Authorized Resellers or in Pindrop's business continuity program, and may be changed, suspended or discontinued by Pindrop at any time with prior notice to you. Except as expressly indicated otherwise in a written notice from Pindrop or the Documentation for a given Pre-GA Offering, your access and use of a Pre-GA Offering are limited to your employees and the Authorized Geography, and is solely for internal evaluation and/or testing purposes, and is subject to any additional terms identified and mutually agreed to by Pindrop and you in writing, including geography or call traffic (i.e., "test" or production calls) restrictions. Either party may terminate your use of a Pre-GA Offering at any time with written notice to the other party.

5. Confidentiality.

(a) **Definition.** "**Confidential Information**" means information designated as confidential or proprietary or that should be considered confidential from its nature or from the circumstances surrounding its disclosure. For clarity, Pindrop Property is Pindrop's Confidential Information, and the Your Call Data is Your Confidential Information.

(b) Use and Disclosure. With respect to any Confidential Information a party receives ("**Receiving Party**") from the other party ("**Disclosing Party**"), Receiving Party will: (i) keep the information confidential; (ii) use the same degree of care for the Disclosing Party's Confidential Information that it uses for its own Confidential Information, but in no event less than reasonable care; (iii) not use the Confidential Information other than in connection with the performance of this TOS and each Reseller Order; and (iv) not divulge the Confidential Information to any third party. Receiving Party agrees to use all reasonable steps to ensure that the Disclosing Party's Confidential Information is not disclosed by a Receiving Party Representative (defined below) in violation of this Section. You also agree that you will not disclose the results of benchmark tests or any other evaluation of any Pindrop Property to any third party without Pindrop's prior written approval. For purposes of this Section, "third party" does excludes Receiving Party and its affiliates employees, contractors, subcontractors attorneys, accountants or other professional advisors of the Receiving Party, as long as the representative (1) has a commercially reasonable need to know and access the Confidential Information in connection with the authorized purposes; and (2) is under contractual or fiduciary confidentiality obligations substantially equivalent to the terms and conditions of this Section (each a "**Representative**"). Receiving Party is responsible for its Representatives' breach of the confidentiality obligations in this TOS to same extent as the Receiving Party itself.

(c) **Exclusions.** Confidential Information does not include information that: (i) is or becomes generally known or available to the public at large other than as a result of a breach by the Receiving Party of any obligation to the Disclosing Party; (ii) was known to the Receiving Party free of any obligation of confidence prior to disclosure by the Disclosing Party; (iii) is disclosed to the Receiving Party on a non-confidential basis by a third party who did not owe an obligation of confidence to the Disclosing Party; or (iv) is developed by the Receiving Party independently of and without reference to any part of the Confidential Information. Confidential Information will not be deemed to be in the public domain or generally known or available to the public merely because any part of said information is embodied in general disclosures or because individual features, components or combinations thereof are now or become known to the public. During the Term, Receiving Party may publicize the existence of the relationship between Pindrop and you in connection with Products or Services provided under a Reseller Order, and Pindrop may list your name on Pindrop's standard customer lists.

(d) Limited Exceptions. Confidential Information may be disclosed in response to a valid order by a court or other governmental body of the United States or any political subdivision thereof, as otherwise required by law, or as necessary to establish the rights of either party under this TOS, provided that the party making the disclosure must provide written notice to the other party prior to the disclosure to provide the other party a reasonable opportunity to obtain a protective order or otherwise protect the confidentiality of the information.

6. Proprietary Rights and Licenses.

(a) Use of Your Call Data. You grant Pindrop, its affiliates and applicable subcontractors a limited-term license to collect, use, record, host, transmit and process Your Call Data as necessary to provide, maintain and support the Product for you in accordance with this TOS, each Reseller Order and the applicable Documentation.

(b) Your Use Rights. Subject to the terms of this TOS, Pindrop hereby grants you a limited, non-exclusive, non-transferable (except as expressly provided in this TOS with respect to the entire agreement) right (i) during the applicable Subscription Term to access and use a Product solely within the Authorized Geography; and (ii) during and after expiration of the applicable Subscription Term to retain and use the portion of the Outputs that are available via the outbound API feeds from the Product solely for your internal business and recordkeeping purposes; provided that (A) the Outputs remain the Confidential Information of Pindrop and subject to the obligations of confidentiality and use restrictions set forth in this TOS; and (B) you will not create any derivative works nor use the Outputs to create a competing solution.

For clarity, to the extent Your Call Data (such as the phone number of a caller) is contained in an Output, nothing in this Section restricts your right to use your own Your Call Data in any manner.

(c) Data Privacy Terms. The terms in Exhibit A (Data Privacy Terms) of this TOS apply.

(d) Support Terms. Pindrop uses Support Tools. Notwithstanding anything to the contrary in this TOS, and subject to the use restrictions below, you agree that Pindrop can also collect, analyze, retain and use the usage, statistical, caller phone number, metadata, and other log data collected by Support Tools or Products ("**Support Data**") to maintain, develop, manage, administer and improve Pindrop's products and services, including the Products and Services and the AI Systems and AI Models ("**Product Improvement Purposes**"). Except where Pindrop is using the Support Data for your sole benefit in its provision of the Products and Services to you, Pindrop will only use the Support Data for Product Improvement Purposes if the Support Data has been aggregated with other comparable data from other customers and then implemented by Pindrop as a general, customer-agnostic improvement to the general usability or efficacy of Pindrop's products and services (i.e., in a manner that does not identify you or any individual person within your company as the source of that data or any individual or phone number of an individual who called you for the benefit of other customers). Pindrop will not and will take reasonable measures to prevent the use of Support Data as an input into any publicly available generative artificial intelligence or machine learning models. You agree that Pindrop's right to retain and use Support Data for Product Improvement Purposes survives any termination or expiration of this TOS or any Reseller Order. You are responsible for disclosing to and obtaining consent from your Users to the collection and use of Support Data, as required by applicable Laws.

For purposes of this TOS,

"**AI**" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to: (i) perceive real and virtual environments; (ii) abstract such perceptions into models through analysis in an automated manner; and (iii) use model inference to formulate options for information or action.

"**AI Model**" means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

"**AI System**" means any data system, algorithm, software, hardware, application, tool, or utility that operates in whole or in part using AI.

"**Machine Learning**" means a set of techniques that can be used to train AI algorithms.

(e) **Implementation and Product-Specific Terms.** The implementation-related and product-specific terms in Exhibit B (Implementation and Product-Specific Terms) apply, as relevant.

(f) **Pindrop Property.** Subject to the limited rights expressly granted by Pindrop under this TOS, Pindrop, its affiliates, and their licensors and third party providers retain and own all right, title, and interest in the Products (including Outputs, AI Systems, and AI Models), the Services (including Work Product) and all updates, upgrades, derivative works, modifications, conversions, improvements or the like made to each of the foregoing, together with all intellectual property rights embodied therein (collectively, the "**Pindrop Property**"). "). If Your Call Data (such as a caller's phone number) is contained in an Output, AI System or AI Model, nothing in this Section transfers or otherwise restricts your ownership in or right to use Your Call Data in any manner. You agree to retain and reproduce all copyright, trademark and other proprietary notices contained on or in the Pindrop Property as delivered to you on all copies of Pindrop Property and will not seek to remove any notices.

(g) Your Property. Subject to the limited rights expressly granted by you under this TOS or a Reseller Order, you retain and own all right, title and interest in all intellectual property rights in and to the Your Call Data, Your Phone Numbers, and Your Call Center Infrastructure.

(h) **Feedback.** You may, at your sole election, provide Feedback to Pindrop or its affiliates to help identify ways in which Pindrop or its affiliates may improve or expand their product and service offerings for their customers. If provided, you agree to assign and hereby assign to Pindrop all right, title and interest in and to the Feedback.

7. Your Warranties. You warrant, acknowledge and agree that (i) you will, on your own behalf and on Pindrop's behalf as your service provider, provide all required consumer notices and disclosures and, where required, secure consents in compliance with all applicable Laws with respect to the Outputs and Your Call Data; and (ii) you will have and maintain privacy policies and terms and conditions with your customers that are compliant with its obligations and applicable Laws and permit the use and sharing of information processed, analyzed or created by a Product (including the creation of Outputs) and/or contributed to the Pindrop Database as contemplated in TOS or a Reseller Order (collectively, the responsibilities under (i) and (ii) are the "**Customer Commitments**"). If you are a "Financial Institution" under the Gramm-Leach-Bliley Act ("**GLBA**"), then (A) you further warrant that your Customer Commitments are also compliant with your obligations as a Financial Institution under the GLBA and (B) you hereby appoint Pindrop, for the duration of your access to and use of Products and Services, as your special agent with limited authority to perform functions inherent in the Products and Services as necessary for you to analyze Calls for the purposes of (1) protecting you and your customers from fraud and (2) enhancing the security of customer transactions. Other than the foregoing appointment in (B), Pindrop has no right, power, or authority to bind you or create obligations on your behalf. If Pindrop, in its good faith judgement, believes that Products are being used in a manner that does not comply with applicable Laws or that could result in noncompliance with applicable Laws, or that could subject you or Pindrop to a claim for liability for noncompliance, Pindrop reserves the right to modify any Products and Services as deemed reasonably necessary to address the noncompliance. You agree to cooperate with Pindrop to the extent reasonably necessary to effectuate the modifications.

8. Limited Warranties. EXCEPT AS PROVIDED OTHERWISE IN THIS TOS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, PINDROP PROPERTY IS PROVIDED TO YOU "AS IS," AND PINDROP, ITS AFFILIATES, AND THEIR LICENSORS AND THIRD-PARTY SERVICE PROVIDERS DISCLAIM ANY AND ALL OTHER PROMISES, REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, QUIET ENJOYMENT, SYSTEM INTEGRATION AND/OR DATA ACCURACY. PINDROP, ON BEHALF OF ITSELF, ITS AFFILIATES, AND THEIR LICENSORS AND THIRD-PARTY SERVICE PROVIDERS, DOES NOT WARRANT THAT PINDROP PROPERTY WILL MEET YOUR REQUIREMENTS, THAT THE

OPERATION OR USE OF THE FOREGOING WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL ERRORS WILL BE CORRECTED. YOU ACKNOWLEDGE AND AGREE THAT THE DISCLAIMERS, LIMITATIONS, AND EXCLUSIONS OF LIABILITY IN THIS TOS FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES, AND THAT, ABSENT SUCH DISCLAIMERS, LIMITATIONS AND EXCLUSIONS, THE TERMS OF THIS TOS, INCLUDING, WITHOUT LIMITATION, THE ECONOMIC TERMS, WOULD BE SUBSTANTIALLY DIFFERENT.

9. Limitations of Liability.

(a) **Consequential Damages Waiver.** IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING, BUT NOT LIMITED TO DAMAGES, LOSSES, OR COSTS INCURRED AS A RESULT OF LOSS OF TIME, LOSS OR CORRUPTION OF APPLICATION OR DATA, LOSS OF PRODUCT OR REVENUE, OR LOSS OF USE OF THE PRODUCTS) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT PRODUCT LIABILITY, OR OTHERWISE, EVEN IF THE PARTY HAS BEEN INFORMED OF THE POSSIBILITY OF THOSE DAMAGES IN ADVANCE.

(b) **Direct Damages.** EACH PARTY'S MAXIMUM AGGREGATE LIABILITY TO THE OTHER PARTY FOR DAMAGES ARISING FROM OR RELATED TO THIS TOS OR ANY PINDROP PROPERTY, WHETHER FOR BREACH OF CONTRACT OR WARRANTY, STRICT LIABILITY, NEGLIGENCE OR OTHERWISE, WILL NOT:

(i) FOR PINDROP, EXCEED TWO TIMES THE FEES PAID TO PINDROP BY THE AUTHORIZED RESELLER DURING THE PRECEDING 12 MONTHS FOR THE PRODUCT, WORK PRODUCT OR SERVICE UNDER THE RESELLER ORDER GIVING RISE TO THE LIABILITY; AND

(ii) FOR YOU, EXCEED TWO TIMES THE FEES PAID OR PAYABLE BY YOU TO THE AUTHORIZED RESELLER DURING THE PRECEDING 12 MONTHS FOR THE PRODUCT, WORK PRODUCT OR SERVICES UNDER THE RESELLER ORDER GIVING RISE TO THE LIABILITY.

(c) Exclusions.

(i) The limitations of liability in Sections 9(a) (Consequential Damages Waiver) and 9(b) (Direct Damages) do not apply to (A) a party's infringement or misappropriation of the other party's intellectual property rights, (B) a party's breach of its confidentiality obligations under this TOS, (C) Pindrop's obligations under Section 10(a) (Infringement Claims), and, as a Responsible Party, under Section 10(c) (Procedures for Third Party Claims), or (D) your obligations under Section 10(b) (Your Coverage for Third Party Claims) and, as a Responsible Party, under Section 10(c) (Procedures for Third Party Claims).

(ii) The limitation of liability in Section 9(b) (Direct Damages) does not apply to your breach of Section 7 (Your Warranties) or the PCI Restriction.

10. Responsibility for Third Party Claims.

(A) **Infringement Claims.** Pindrop agrees, at its expense, to defend, indemnify, and hold you harmless from and against any and all third-party claims, actions, demands, legal proceedings, liabilities, damages, losses, judgments, authorized settlements, and reasonable costs and expenses as incurred, including without limitation attorney's fees, where a third party alleges that a Product furnished to you and used within the scope of and in compliance with this TOS infringes a U.S. copyright or any U.S patent issued as of the Effective Date. Pindrop is not responsible under this Section for infringement arising out of or related to: (i) modification of a Product by anyone other than Pindrop, where the Product would not infringe except for that modification, (ii) combination of a Product with other software, hardware, processes, or materials not provided by Pindrop, where the Product would not infringe except for the combination, (iii) Third-Party Software Components, when taken on a stand-alone basis and not in combination with other elements of the relevant Product, (iv) your use of a Product version other than the most recent release if infringement would have been avoided with the use of the most recent release (but only if Pindrop has provided Company access to the most recent release at no additional charge), or (v) Your Call Data, where the Product would not infringe except for Your Call Data. If a Product is held or believed by Pindrop to infringe (and none of the exclusions above apply), Pindrop may, at its sole option and expense, elect to: (A) modify the Product so that it is non-infringing, (B) replace the Product with non-infringing products which are functionally equivalent or superior in performance, (C) obtain a license for you to continue to use the Product as provided in the Reseller Order, or (D) terminate the license for the infringing Product and refund any prepaid but unused license fees paid by Authorized Reseller to Pindrop for the Product under the impacted Reseller Order. THE RIGHTS GRANTED TO YOU UNDER THIS SECTION 10(a) ARE YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM OF INFRINGEMENT OR MISAPPROPRIATION RELATED TO THE PRODUCTS AND THE THIRD-PARTY CLAIMS DESCRIBED IN THIS SECTION 10(a).

(b) Your Coverage for Third Party Claims. You agree, at your expense, to defend, indemnify, and hold Pindrop and its affiliates (each a "**Pindrop Party**") harmless from and against any and all third-party or settle any claims, actions, demands and legal proceedings, liabilities, damages, losses, and judgments or authorized settlements, and reasonable costs and expenses as incurred, including without limitation attorney's fees arising out of or in connection with any alleged or actual breach or violation of (i) Section 7 (Your Warranties), (ii) other applicable Laws for which you are responsible under this TOS in connection with your use of or access to the Products or Services, including the collection, processing, analysis, creation, storage, and retention of Your Call Data and Outputs, and (iii) the PCI Restriction.

(c) Procedures for Third Party Claims. For each party to be responsible for its indemnification obligations under Sections 10(a) (Infringement Claims) or 10(b) (Your Coverage for Third Party Claims), as relevant ("**Responsible Party**"), the other party ("**Covered Party**") must (i) promptly notify Responsible Party in writing of its receipt of notice of any claim or when it discovers facts on the basis of which Covered Party intends to request indemnification (each, a "**Claim Notice**"), (ii) afford the Responsible Party the choice to control the claim's defense and all related settlement negotiations (provided that Covered Party can participate at its own expense), and (iii) provide the Responsible Party with reasonable assistance, information and authority necessary to fulfill its obligations under Sections 10(a) or 10(b) above. Responsible Party will keep Covered Party reasonably informed as to the status of Responsible Party's efforts in connection with the defense or settlement of claims on Covered Party's behalf, and to reasonably consult with Covered Party (or Covered Party's counsel) concerning those efforts.

Notwithstanding anything to the contrary in Section 10(c)(i), Covered Party's failure to provide a Claim Notice does not relieve Responsible Party of its liability to the Covered Party under Sections 10(a) or 10(b) above, as relevant, unless the delay materially prejudices Responsible

Party's defense or the scope of Responsible Party's liability for the relevant third-party claim.

Notwithstanding anything to the contrary in Section 10(c)(ii):

(A) Responsible Party will not, without Covered Party's written approval, make any admission of facts that expose Covered Party to any liability, require Covered Party to take or cease to take any action (including without limitation any requirement to make payments), or expose Covered Party to other claims that are not covered under Section 10. However, if Responsible Party is required by applicable Law to make an admission, Responsible Party may proceed in making the admission without Covered Party's prior approval, provided that Responsible Party notifies Covered Party in writing to afford Covered Party a reasonable opportunity to obtain a protective order or otherwise address the requirement with the appropriate authority.

(B) If Responsible Party fails to respond to a Claim Notice or refuses to assume the defense of a claim tendered in good faith within 10 days of its receipt of a Claim Notice under which Covered Party is seeking indemnification under this Section 10, then Covered Party may proceed to defend or otherwise settle the claim as Covered Party deems reasonably appropriate and Responsible Party agrees to reimburse Covered Party with respect to all defense costs and expenses or damages incurred with respect to the claim, as incurred.

11. Term and Termination.

(a) Term of TOS. The term of this TOS commences on the Effective Date and continues for the duration of the initial Reseller Order ("**Initial Term**"), unless terminated sooner. This TOS automatically renews annually thereafter for additional 3 year periods, unless one party provides the other party no less than 60 days written notice prior the expiration of the then-current year (each a "**Renewal Term**" and together, the Initial Term and Renewal Term are the "**Term**"). This TOS remains binding in full force and effect and continues to apply to any Reseller Orders that have not terminated or expired as of the effective date of termination of this TOS until those Reseller Orders terminate or expire according to their own terms. For clarity, a notice of non-renewal of this TOS does not in any way modify, impact the validity of, or terminate any existing Reseller Orders.

(b) Mutual Rights of Termination. Either party to this TOS may terminate this TOS or a Reseller Order if the other party materially breaches this TOS or a Reseller Order and fails to cure the breach within 30 days of receiving written notice from the non-breaching party ("**Cure Period**") specifying the nature of the breach and the actions required to cure the breach, provided, however, that if the breach does not involve the payment of amounts to Pindrop, and is of a nature that can be cured but not within the Cure Period, and the breaching party has commenced significant efforts to cure the breach within the Cure Period, the TOS or Reseller Order will not terminate so long as the breaching party continues to diligently pursue the completion of the cure.

(c) For Cause Termination. If Pindrop rightfully terminates this TOS pursuant to Section 11(b) (Mutual Rights of Termination), you acknowledge and agree that Pindrop can also instruct Authorized Reseller to immediately terminate the impacted Reseller Order upon written notice to you without liability of any kind incurred by either Pindrop or Authorized Reseller. If you rightfully terminate this TOS under Section 11(b), any corresponding rights you may have to terminate an impacted Reseller Order are as described in the terms of Your Agreement and the Reseller Order.

(d) Obligations Upon Termination. Upon the expiration or termination of this TOS or a Reseller Order for any reason, all rights and licenses granted to you under this TOS and impacted Reseller Orders immediately terminate and you will, at Pindrop's sole option, return or destroy all relevant Pindrop Property. Further, at Disclosing Party's request Receiving Party agrees to (i) destroy Disclosing Party Confidential Information in its possession or control and (ii) confirm to Disclosing Party in writing that Receiving Party has complied with any destruction instructions. However, Confidential Information (A) in Receiving Party's or its Representatives' archives (including legal archives and business records generated in the delivery and support of Products and Services) or back-up or other systems, (B) expressly authorized in this TOS to be retained, or (C) retained to comply with litigation holds or Laws, in each case is required to be destroyed only in accordance with the Receiving Party's and its Representatives' data retention policies, litigation hold or Laws, whichever is the longest of the retention requirements. An Reseller Order may specify additional or different obligations upon termination for a given Product. You understand and agree that Pindrop has no obligation to save or otherwise make all or any portion of the Outputs available after the effective termination date of a Reseller Order. The following terms survive expiration or termination of this TOS or any Reseller Order: this Section 11(d), all defined terms and terms which expressly survive, and the Sections 2 (Engagement Model), 3(b) (Protection of Your Call Data), 5 (Confidentiality), 6(d) (Support Terms), 6(f) (Pindrop Property), 6(g) (Your Property), 6(h) (Feedback), 7 (Your Warranties), 8 (Limited Warranties), 9 (Limitations of Liability), 10 (Responsibility for Third Party Claims), 12 (Audits), and 13 (General).

12. Audits. During the Term for a period of 6 months thereafter, upon reasonable prior written notice to the other party (email is sufficient), each party ("**Auditing Party**") has the right, at its expense, to conduct (or have a third party conduct, or in the case of Pindrop, may also involve the Authorized Reseller) an audit, assessment, examination or review of relevant documentation, materials or systems of the other party ("**Audited Party**") for the sole purpose of assessing Audited Party's compliance with this TOS and each Reseller Order. Audited Party will reasonably cooperate with the request by providing reasonable access to knowledgeable personnel, systems, documentation, and other reasonably requested information. You acknowledge and agree there may be restrictions on your ability to conduct audits on Pindrop's subcontractors.

Audits will not be conducted more than once per year (unless a material non-compliance is detected, in which case an additional audit may be performed to verify that any agreed to corrective actions have been taken). Audits must be conducted during normal business hours and in a manner not to unreasonably disrupt Audited Party's day to day business Any site visit at the Audited Party or audit of Audited Party's procedures, systems and equipment is subject to Audited Party's reasonable policies and practices that are in effect to maintain the security of Audited Party's site, systems, and equipment, and to protect the confidentiality of proprietary and confidential information. Audited Party is not required to give access to or disclose any confidential information of a third party or any attorney-client privileged information.

Auditing Party is not obligated to share audit results with Audited Party. However, the results of any audit are the Confidential Information of both parties, and in all cases subject to the confidentiality obligations in this TOS.

13. General.

(a) **Export Compliance.** The Pindrop Property and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Each party represents that it is not on any U.S. government denied-party list. You will not permit any User to access or use any Pindrop Property in a U.S.-embargoed country or

region (currently Cuba, Iran, North Korea, Syria or Crimea) or in violation of any U.S. export law or regulation or other equivalent laws of other jurisdictions, as applicable.

(b) **Governing Law; Jurisdiction and Attorneys' Fees.** This TOS will be governed by and construed in accordance with the laws of the State of Delaware, without regard to its conflict of law provisions. With respect to any legal disputes between you and Pindrop arising out of or related to this TOS, you and Pindrop irrevocably consent to the exclusive personal jurisdiction of the federal courts located in Delaware or, if the Federal courts do not have jurisdiction, in the Superior Court of the State of Delaware, and any appellate court from any state or Federal court. In the event of any dispute arising out of or related to this TOS, the prevailing party is entitled to recover its reasonable attorneys' fees and costs.

(c) Notices. All notices permitted or required under this TOS will be in writing and will be delivered as follows with notice deemed given as indicated (i) by personal delivery when delivered personally; (ii) by commercially established courier service upon delivery or, if the courier attempted delivery on a normal business day and delivery was not accepted, upon attempted delivery; or (iii) by certified or registered mail, return receipt requested, 10 days after deposit in the mail. Notice will be sent to the parties at the addresses as each party will notify the other of in writing or, in the case of Pindrop, it can rely on the address on record with the Authorized Reseller for notification purposes. Pindrop's notice information is as follows: Pindrop Security, Inc., Attn: Legal Department, 1115 Howell Mill Road NW, Suite 700, Atlanta, GA 30318, with copy to: generalcounsel@pindrop.com.

(d) Waivers; Severability. Neither party will by mere lapse of time without giving notice or taking other action be deemed to have waived any breach by the other party of any of the provisions of this TOS. Further, the waiver by either party of a particular breach of this TOS by the other party will not be construed as, or constitute, a continuing waiver of the breach, or of other breaches of the same or other provisions of this TOS. If any provision of this TOS is held illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this TOS, the validity of the remaining provisions are not affected.

(e) Force Majeure. Except for the payment of money due or payable, neither party is liable for any failure or delay in performance under this TOS which might be due to strikes, shortages, riots, insurrection, fires, flood, storm, other weather conditions, explosion, acts of God, war, government action, inability to obtain delivery of parts, supplies or labor, labor conditions (including strikes, lockouts or other industrial disturbances), earthquakes, riots or acts of terrorism, epidemic, pandemic or any other cause which is beyond the reasonable control of the party (each a "force majeure event"). The occurrence of a force majeure event does not relieve Pindrop of its obligation to implement its disaster recovery plan or provide disaster recovery services with respect to an impacted Product, as contemplated in Section 11 (BCP Program) of Exhibit C (Pindrop Information Security and BCP Programs) attached.

(f) **Assignment.** This TOS may not be assigned or transferred without the prior written consent of Pindrop. Pindrop may assign this TOS to any third party who succeeds to substantially all of Pindrop's assets and business related to the Products by merger or purchase, provided that the assignee assumes this TOS by an instrument in writing.

(g) **Entire Agreement.** This TOS is the complete agreement between the parties with respect to its subject matter and supersedes any and all prior agreements and understandings, and may be amended only in a writing that refers to this TOS and is signed by both parties. The parties are independent contractors. Except as expressly agreed by the parties, neither party is deemed to be an employee, agent, partner or legal representative of the other for any purpose and neither will have any right, power or authority to create any obligation or responsibility on behalf of the other. To the extent of any conflict between this TOS and Your Agreement or any Reseller Order, this TOS controls.

(h) **Injunctive Relief.** Notwithstanding any other provision of this TOS, any violation by either party to this TOS of the other party's intellectual property or proprietary rights will cause irreparable damage for which recovery of money damages would be inadequate, and the aggrieved party will therefore be entitled to seek timely injunctive relief to protect the party's rights, without the need to post bond.

(i) **Limited Right to Modify.** If litigation or a change in Law occurs that affects this TOS or either party's activities under this TOS, and a party reasonably believes in good faith that the litigation or change will have a substantial adverse effect on that party's rights or obligations under this TOS, then the party may, upon written notice, require the other party to renegotiate or supplement the terms of this TOS in good faith. The notice must reasonably detail the nature of the proposed modifications. Pindrop may also, at its discretion, modify this TOS as necessary to account for new Product features or functionality or new Services it plans to make generally commercially available to its customers ("**Product/Service Update**"). Product/Service Updates are effective no sooner than 60 days after Pindrop notifies you or Authorized Reseller of the same via email ("**Product/Service Notice Period**"). If Pindrop issues a written notice to you to modify this TOS under this Section, you agree to notify Pindrop in writing of any objections to the proposed changes within 30 days of receiving the notice. If you do not object to a Product/Service Update within the Product/Service Notice Period, then the changes are deemed accepted. Notwithstanding the foregoing, if the Product/Service Update is not material or is beneficial to you, the Product/Service Update is effective immediately upon Pindrop's written notice to you (without the process described above).

EXHIBIT A

Data Privacy Terms

1. Definitions.

(a) "**Aggregate Data**" means information that relates to a group or category of individuals, from which individual identities have been removed, that is not linked or reasonably linkable to any individual or household.

(b) "**Data Protection Laws**" means any state or federal privacy or data protection laws to which you or Pindrop (as a service provider to you) are subject, including but not limited to, the Gramm-Leach-Bliley Act (GLBA) and its implementing regulations; the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), Cal. Civ. Code 1.81.5, the Utah Consumer Privacy Act (UCPA), Utah Annotated Code §13-61-101, the Virginia Consumer Data Protection Act (VCDPA), Va. Code Ann. §§ 59.1-575 to 59.1-585, and any other legislation which implements any other current or future legal act concerning the protection, privacy, and/or processing of Personal Data, including any amendment or re-enactment of the foregoing.

(c) "**Deidentified Data**" means information that cannot reasonably identify, related to, described, be capable of being associated with, or linked, directly or indirectly, to a particular individual.

(d) "**Personal Data**" means any personal information as described in the applicable Data Protection Laws and relates only to Personal Data, or any part of the Personal Data, in respect of which Pindrop is a processor in connection with the performance of its obligations under the TOS.

(e) "**Process**", "**Processing**", or "**Processed**" means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether automated or not, such as, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(f) "**Processing Purpose**" means the purpose for which Pindrop is Processing Personal Data as set forth in Section 2(b) of this Exhibit A.

(g) "**sale**", "**sell**", or "**selling**" will have the meaning as ascribed to it under applicable Data Protection Law.

(h) "**Business**", "**Controller**", "**Processor**", and "**Service Provider**" will have the meaning as ascribed to it or to a similar term under applicable Data Protection Law.

2. Processing Purpose. With respect to Pindrop's provision of the Products and Services to you pursuant to this TOS and each Reseller Order ("Relevant Agreements"):

(a) Pindrop is a Service Provider or Processor (as applicable), with respect to any Personal Data that Pindrop Processes, on your behalf, pursuant to the Relevant Agreements ("**Personal Data**");

(b) You have disclosed Personal Data to Pindrop and its affiliates for the Processing Purposes of (1) detecting security incidents and/or utilization by a caller of a non-human voice, and protecting against malicious, deceptive, fraudulent or illegal activity (including, in each case, populating the Pindrop Database); and (2) assisting in the authentication of your callers, as well as is reasonably necessary in support of any other valid Processing Purposes that are part of the Products, Services and that are expressly agreed to by the parties in the Relevant Agreements, including and subject to restrictions on use such as those applicable to Fraudulent Call Data;

(c) Pindrop and you acknowledge and confirm that Pindrop does not receive any Personal Data as consideration for any Products, Services or other items provided under the Relevant Agreements; and

(d) You hereby instruct and authorize Pindrop to Process Personal Data in connection with Pindrop's performance and exercise of its obligations and rights under the Relevant Agreements. Any additional or alternate instructions must be mutually agreed upon in writing.

3. Permitted Use. Pindrop will only collect, use, retain, disclose and otherwise Process Personal Data: (a) for its performance of the Relevant Agreements and the Services and provision of the Products, including in support of Pindrop's and its affiliates internal operations as necessary to the provision of the Products and Services; (b) for its internal use to build or improve the quality of the Products and Services, provided that Pindrop does not use the Personal Data to perform services on behalf of another person; or (c) as otherwise necessary for compliance with applicable Laws. Pindrop will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and are subject to a duty of confidentiality with respect to Personal Data.

4. Service Providers. Pindrop may disclose Personal Data to, and permit the Processing of Personal Data by, its service providers who perform services on behalf of Pindrop, in support of the provision of the Products and Services to you (each a "Service Provider"). Pindrop will ensure that the Service Providers are subject to equivalent contractual requirements with respect to Personal Data that apply to Pindrop under this Exhibit A. Pindrop will be responsible for the actions of its Service Providers that breach the terms of this Exhibit A.

5. Restrictions. Pindrop is prohibited from selling, retaining, using, disclosing, or otherwise Processing Personal Data for any purpose other than for the Processing Purpose or as otherwise set forth in Section 6 (Deidentified Data and Aggregated Data) of this Exhibit A, which, for the avoidance of doubt, also prohibits Pindrop from retaining, using, or disclosing Personal Data outside of its business relationship with you or for any other Commercial Purpose. Where permitted by you under the Relevant Agreements, Pindrop may retain use, or otherwise Process certain Personal Data (and combine it with personal data from other clients) as reasonably necessary to detect data security incidents, or protect against fraudulent or illegal activity (e.g., as part of the Pindrop Database). Pindrop certifies that it understands and will comply with the foregoing restrictions set forth in this paragraph.

6. Deidentified Data and Aggregate Data. Pindrop and its affiliates may use Deidentified Data and Aggregate Data relating to Personal Data or derived from the Products and Services, for the purposes of providing the Products and Services, improving its operations, and enhancing the features, functions, and performance of the Products and Services. Pindrop and its affiliates may also, during and after the term of the TOS, use, maintain, and disclose the Deidentified Data and Aggregate Data for its own product improvement and general purposes. Pindrop will not identify you

or otherwise disclose you as the source of any Deidentified Data or Aggregate Data in connection with any general use purposes. For clarity, Support Data may, if it meets the criteria set forth in this Section 6, also be used for the purposes authorized in this Section.

7. Audit. You will have the right to audit Pindrop's Processing of Personal Data and Pindrop's compliance with this Exhibit A in accordance with Section 12 (Audits) of the TOS. Any report, documents, information, or record provided to you or created pursuant to this Section 7 are considered Pindrop Confidential Information.

8. Duration of Processing. Pindrop will only Process Personal Data for the duration of the Relevant Agreements and as otherwise allowed under the Relevant Agreements or permitted under applicable Law. Unless retention of Personal Data is otherwise permitted under the Relevant Agreements, at the termination or expiration of the Relevant Agreements, Personal Data will be returned and/or deleted in accordance with Section 11(d) (Obligations Upon Termination) of the TOS.

9. Data Subject Requests. If Pindrop receives a complaint, dispute, or request from a data subject to exercise the data subject's rights under Data Protection Laws, and Pindrop is able to confirm that the request relates to you, Pindrop will promptly notify you of the data subject request. Taking into account the nature of Pindrop's Processing of Personal Data, Pindrop will provide reasonable assistance to you in responding to data subject requests as required by Data Protection Laws and only to the extent commercially feasible. Unless required by applicable Law, Pindrop will not respond to or take any action to comply with a data subject request without your approval.

EXHIBIT B

Implementation and Product-Specific Terms

1. Call Routing. The Product will be implemented and deployed based on an agreed to architecture for the routing of calls ("Approved Architecture"). The Approved Architecture will apply for the duration of the applicable Subscription Term, unless Pindrop, the Authorized Reseller and you mutually agree otherwise in writing.

2. Pindrop Protect Cloud-Specific Terms.

(a) **Pindrop Database.** During the term of a Reseller Order, the Product will collect, process, and analyze Your Call Data. Pindrop and its affiliates are authorized to use and contribute the Fraudulent Call Data to the Pindrop Database for the purpose of identifying, monitoring and tracking phone-based fraud and suspicious transactions or passively authenticating a caller for the purpose of identifying, monitoring and tracking phone-based fraud and suspicious transactions or passively authenticating a caller for the benefit of you, Pindrop's and its affiliates' existing or future customers, and the Consortium Members ("**Authorized Use of Fraudster Data**"). Pindrop will only identify (i.e., "tag") that the Fraudulent Call Data was provided by you on a pseudonymized basis (e.g., using a code name within the Pindrop Database itself). For clarity, neither you nor any other customer of Pindrop has or will have access to or the ability to view the Pindrop Database or the data stored therein. You agree that the Authorized Use of Fraudster Data will survive any termination or expiration of this TOS and the applicable Reseller Orders.

(b) Call Recording Storage Terms. The following call recording storage and related terms will apply to the configuration reflected in the applicable Reseller Order:

Your Storage of Your Call Recordings (default configuration unless specified otherwise in the applicable Reseller Order)

The default storage option for call recordings created by a Product in the ordinary course of its use is the use of your own Core Hosting Provider (as defined below) instance (i.e., under your own direct account with the Core Hosting Provider) (each a "**CHP Instance**"). For purposes of this Exhibit B, "**Core Hosting Provider**" or "**CHP**" means the third-party service provider whom Pindrop uses to host the Products covered under a Reseller Order (e.g., AWS or Google), as reflected in the relevant Reseller Order.

You are solely responsible for all aspects of Your CHP Instance, including without limitation, the cost of securing and maintaining Your CHP Instance for the duration of the Reseller Orders as well as the security settings applicable to Your CHP Instance.

Your CHP Instance will be configured for use with a Product as set forth in the Approved Architecture, which configuration will include, at a minimum, (i) sufficient administrative and access rights for Pindrop to be able to monitor and maintain the call recordings as needed to deliver the Product as contemplated in the Documentation and for the Authorized Reseller and Pindrop to provide the maintenance and support for that Product (including sharing your share IAM credentials including access key, secret key and encryption settings with Pindrop for the duration of the applicable Subscription Term to enable access); and (ii) the retention of the call recordings for the Calls as established from time to time based on your instructions and the standard features and functionality of the Product (collectively, "**Minimum CHP Configuration Requirements**"). You agree to maintain the Minimum CHP Configuration Requirements for Your CHP Instance for the duration of all Reseller Orders applicable to the Product, unless you, Pindrop and the Authorized Reseller mutually agree otherwise in writing.

Upon the expiration or termination of your right to use a Product under a Reseller Order, you are responsible for the deletion of any call recordings from Your CHP Instance.

Pindrop Storage of Call Recordings

If the parties agree as part of the Approved Architecture that Pindrop, rather than you, will store the call recordings created by the Product in its ordinary course of use on your behalf in Pindrop's CHP instance (i.e., under Pindrop's own and direct account with the CHP) ("**Pindrop CHP Instance**"), then the following terms apply:

Pindrop will maintain the call recordings based on the time periods configured within the Product as established from time to time based on your instructions and the standard features and functionality of the Product.

Your Named Users will have access to the call recordings through the standard user interface for the Product to enable Named Users to disposition a given Call as either fraudulent or genuine. No other administrative access will be granted to you for the Pindrop CHP Instance.

Upon the expiration or termination of your right to use a Product under a Reseller Order, Pindrop will delete any remaining call recordings from the Calls from Pindrop's CHP Instance.

3. Amazon Connect Integration Specific Terms. Where the Implementation Model for the Product will use Pindrop's native integration call capture method for Amazon Connect, the term "Your Call Data" includes the Amazon Connect Data Stream (i.e., the call audio, Contact Status Request, Contact Trace Record Stream and Agent Event Stream and any replacement features and functionality that collect or create data within Amazon Connect for a given Call and are then routed by Amazon Connect to the Product for analysis). Currently, AWS refers to these more generally as the "Kinesis" data streams and the AWS Lambda functions.

4. Call Center Partner Integration-Related Terms. This Section applies if the Implementation Model for the Product will use a call capture method that integrates with a Call Center Partner Solution (as reflected in the relevant Reseller Order). As your subcontractor with access to the Product, you are responsible for compliance of the Call Center Partner and the Call Center Partner Solution with the terms of this TOS and each Reseller Order to the same extent as your own personnel and systems.

For purposes of this Section:

"**Call Center Partner**" means the third-party vendor used by you to provide your contact center through which the Calls will be routed, as further detailed in the applicable Implementation Model. Examples of Call Center Partners include Amazon with respect to Amazon Connect and Twilio with respect to Twilio's call center offerings.

"**Call Center Partner Solution**" means the solution and services that are obtained by you from the Call Center Partner under a direct agreement between you and the Call Center Partner.

5. Acceptable Use Policy. With respect to your transmission of Your Call Data via the Product, you agree to comply with Pindrop's then-current acceptable use policy (available upon

request or at https://www.pindrop.com/wp-content/uploads/2021/12/Pindrop-Acceptable-Use-Policy-Sept-2018.pdf).

6. CHP Flow-Down Terms. In providing hosting and related cloud platform services ("CHP Services") to you, and notwithstanding anything to the contrary in this TOS, the following terms apply to CHP Services. You acknowledges and agree that (a) the CHP may require that Pindrop notify it of your unauthorized access or use of CHP Services, and you hereby authorize Pindrop to provide any required notice to the CHP, (b) your receipt of the CHP Services may be subject to legal intercept or monitoring activities by CHP, its suppliers, or local authorities in accordance with its standard business practices and applicable Laws, and (c) you may not use the CHP Services, or any interface provided with the CHP Service, to access or use any other CHP product or service in a manner that violates the terms of service applicable to the other CHP product or service.

7. Tap-To-Cloud Call Capture Terms. If the call capture method for the Product is specified as "tap-to-cloud" in a Reseller Order, then the additional terms in Exhibit D (TTC Appliance Terms) apply.

EXHIBIT C

Pindrop Information Security and BCP Programs

Last Updated: February 3, 2023

1. Definitions.

Capitalized terms used in this Exhibit C have the meanings given below or, if not defined below, the meanings given in this TOS or its other Exhibits.

"Appliances" means all appliances (including, without limitation, Pindrop's or Pindrop-provided Products) that you procure under a Reseller Order and install within your facilities, your data centers, or your third-party data centers.

"In-Scope Subcontractor" means a subcontractor who Pindrop engages to deliver components of Products or Services to you and who will have access to, process, or store Your Call Data.

"**Information System**" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

"**Pindrop-Controlled Information Systems**" means: (i) Information Systems that are within Pindrop's possession or control; and (ii) Amazon Web Services ("**AWS**") or Google Cloud Platform ("**GCP**") or Information Systems that are: (a) under Pindrop's enterprise account with AWS or GCP; (b) used by Pindrop to deliver the Products or Services or used by Pindrop for Pindrop's internal, corporate-level systems; and (c) are AWS or GCP Information Systems for which Pindrop solely configures and manages the security controls used by Pindrop to protect the data stored within those Information Systems. For clarity, "Pindrop-Controlled Information Systems" excludes all of Your Information Systems.

"Regulator" means any industry regulatory agency with supervisory authority over your company under applicable Laws.

"**Security Breach**" means a reasonably suspected or confirmed unauthorized disclosure of your Confidential Information within Pindrop's possession or control; or a reasonably suspected or confirmed unauthorized access by a third party to any Pindrop-Controlled Information Systems that process, hold, or provide access to your Confidential Information.

"**Your Information System**" means (i) Information Systems that are within your possession or control and (ii) all Appliances.

2. Governance and Oversight.

(a) Pindrop will have in place a cybersecurity program designed to protect the confidentiality, integrity, and availability of the Pindrop-Controlled Information Systems, as detailed in this Exhibit C. Such cybersecurity program includes tracking data asset locations and maintaining risk based written security policy or policies that satisfy the requirements set forth in this Exhibit C ("**Security Policy**"). Pindrop will not make any change to its Security Policy that will materially degrade the overall level of security described in this Exhibit C.

(b) Pindrop's Security Policy will be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of your Confidential Information within Pindrop's possession or control that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of the information, and assesses the sufficiency of any safeguards in place to control these risks. The risk assessment will be written and include: (i) criteria for the evaluation and categorization of identified security risks or threats to your Confidential Information within Pindrop's possession or control; (ii) criteria for the assessment of the confidentiality, integrity, and availability of your Confidential Information within Pindrop's possession or control, including the adequacy of the existing controls in the context of the identified risks or threats; and (iii) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the Security Policy will address the risks.

(c) Pindrop will periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of your Confidential Information within Pindrop's possession or control that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of the information, and reassess the sufficiency of any safeguards in place to control these risks.

(d) Pindrop will (i) design and implement safeguards to control the risks identified through the risk assessments it performs; and (ii) evaluate and adjust its information security program in light of the results of the testing and monitoring described in this Exhibit C, any material changes to Pindrop's operations or business arrangements, and any other circumstances that Pindrop knows or has reason to know may have a material impact on Pindrop's information security program.

(e) Pindrop will assign an appropriate individual within Pindrop's Information Security team to maintain responsibility and executive oversight for the Security Policy, including, without limitation, implementation, formal governance and revision management, employee education, and compliance enforcement. The individual assigned by Pindrop to maintain responsibility and executive oversight for the Security Policy will report in writing, regularly and at least annually, to Pindrop's executive team or board of directors or equivalent governing body. Any reports will include the following information: (i) the overall status of Pindrop's information security program; and (ii) material matters related to Pindrop's information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, compliance obligations and recommendations for changes in the information security program.

(f) Subject to the terms and conditions in Section 12 (Audits) of the main body of the TOS, the rights in this Section 2(f) apply. If a Regulator exercising its supervisory authority makes a request to you to access the Products or Services, you will use commercially reasonable efforts to resolve that request directly with the Regulator using alternative methods, including by reviewing the security certifications for the Pindrop-Controlled Information Systems with the Regulator. If

the Regulator determines that the information available through these mechanisms is insufficient to verify compliance with applicable Laws then, upon the Regulator's request and your written confirmation that the Regulator has the requisite supervisory authority over your company to make the request, Pindrop will provide the Regulator with: (i) information about the Products and Services and the opportunity to discuss the Products and Services operations and controls with Pindrop subject matter experts; and (ii) if required, a direct right to examine the Products and Services used by you, including by conducting an examination on premises. Pindrop may charge you a fee (based on Pindrop's reasonable costs) for the discussion, communication, and examination. Any discussion, communication, or examination requested by the Regulator under this subsection will, except in an emergency or crisis situation, be conducted consistent with the terms of Section 12 (Audits) of the main body of the TOS.

3. Policies and Procedures.

(a) The policies that comprise the Security Policy are commercially reasonable, communicated to relevant Pindrop employees, and designed to: (i) be protective of your Confidential Information within the Pindrop-Controlled Information Systems; and (ii) support Pindrop's compliance with its obligations under the TOS. If requested by you in writing, Pindrop agrees to provide you with (1) the title page and table of contents related to the Security Policy or other related policies or procedures applicable to Pindrop's business operations set forth in this Exhibit C; (2) an opportunity to discuss Pindrop's security measures; (3) confirmation that penetration testing and vulnerability scanning has been performed; and (4) independent audit reports applicable to the Products (such as SOC2 Type 2) that Pindrop makes generally available to its customers under confidentiality terms.

(b) Pindrop will review its Security Policy at least annually and amend the Security Policy (or subparts thereof) as Pindrop deems commercially reasonable (e.g., in light of relevant risk assessment findings, relevant changes in applicable laws or standards, technology advances, changes to Pindrop's systems or Pindrop's own changing business operations).

(c) As part of the Security Policy, Pindrop will have security-minded development practices for applications that form any part of the Products or that are used to deliver the Products, and procedures for evaluating and assessing the security of externally developed applications that form any part of the Products or that are used in the delivery of the Products.

(d) Pindrop will maintain and follow employment verification requirements for all new Pindrop employee hires, with the verifications occurring prior to the date of hire. These requirements will include criminal background checks, proof of identity validation, and additional checks as deemed reasonably necessary by Pindrop and as permitted by applicable Law. Such employment verification measures will be in line with requirements under Industry Standards (as defined in Section 4 (Compliance) below). Each Pindrop local entity is responsible for implementing the foregoing requirements in its hiring process as applicable and permitted under local law. Pindrop will provide verification of the completion of background checks in a satisfactory manner for employees upon your reasonable request; however, Pindrop is not required to provide an actual copy of the background check results.

(e) Pindrop will have a training program that includes conducting security education for its employees annually. The training program will: (i) provide security awareness training that is updated to reflect risks identified by Pindrop's risk assessments; and (ii) promote the maintenance of current knowledge of changing information security threats and countermeasures.

4. Compliance. Pindrop-Controlled Information Systems will be subject to annual certification of compliance with the Payment Card Industry Data Security Standards (PCI-DSS) (with respect to relevant cardholder data environments only), ISO 27001, and SSAE SOC 2 or any substantially equivalent or alternative successor standard (the "Industry Standards"). Upon written request from you, Pindrop will provide evidence of the compliance and accreditation with the Industry Standards as reasonably determined by Pindrop, such as certificates, attestations, or reports resulting from accredited independent third-party audits (accredited independent third-party audits will occur at the frequency required by the relevant standard). Additionally, Pindrop will use commercially reasonable efforts to verify that its In-Scope Subcontractors comply with all Laws applicable to the operation of the In-Scope Subcontractors' business and all Laws generally applicable to providers of information technology services, in each case, to the extent relevant to the specific products and services being provided by the In-Scope Subcontractor to Pindrop in connection with the Products and Services covered under the TOS and a Reseller Order. The verification may be accomplished through Pindrop's vendor due diligence process. In the event that Pindrop's vendor due diligence process identifies a non-compliance with the aforementioned Laws, Pindrop will work with the In-Scope Subcontractor to cure the deficiency.

5. Incident Response and Security Breaches.

(a) Pindrop will maintain and follow documented incident response policies consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines or equivalent industry standards for computer security incident handling. Pindrop's written incident response plan will be designed to promptly respond to, and recover from, any event materially affecting the confidentiality, integrity, or availability of your Confidential Information within Pindrop's possession or control. Such incident response plan will address the following areas: (i) the goals of the incident response plan; (ii) the internal processes for responding; (iii) the definition of clear roles, responsibilities and levels of decision-making authority; (iv) external and internal communications and information sharing; (v) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; (vi) documentation and reporting; and (vii) the evaluation and revision as necessary of the incident response plan.

(b) Pindrop will investigate Security Breaches (and security incidents that are not yet Security Breaches but that are reasonably likely to result in Security Breaches) of which Pindrop becomes aware, perform a root-cause analysis of the same and take prompt action designed to contain the Security Breach. You must notify Pindrop of any suspected vulnerability or security incident by immediately submitting a technical support request to Pindrop.

(c) Pindrop will notify you within no more than 24 hours after Pindrop becomes aware of a Security Breach that has impacted your Confidential Information. Pindrop will provide you with reasonably requested information about the Security Breach and the status of any Pindrop containment and service restoration activities.

6. Physical Security and Entry Control.

(a) Pindrop will maintain reasonable physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, designed to protect against unauthorized entry into Pindrop-managed facilities (i.e., its headquarter facility) used to

provide the Pindrop-Controlled Information Systems. Auxiliary entry points into the facilities, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

(b) Access to Pindrop-managed facilities and controlled areas within those facilities will be limited by job role and subject to authorized approval. Such access will be logged, and the logs will be retained for not less than one year. Pindrop will revoke access to Pindrop-managed facilities upon separation of an authorized employee. Pindrop will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.

(c) Any person granted temporary permission to enter an Pindrop-managed facility or a controlled area within the facility will be registered upon entering the premises and will be escorted by authorized personnel.

(d) Pindrop will take precautions designed to protect the physical infrastructure of Pindrop-managed facilities against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

7. Access, Intervention, Transfer and Separation Control.

(a) Pindrop will maintain measures for Pindrop-Controlled Information Systems that are designed to logically separate and prevent your Confidential Information stored within Pindrop-Controlled Information Systems from being exposed to or accessed by unauthorized persons. Pindrop will maintain isolation of its production and non-production environments, and, if your Confidential Information is transferred to a non-production environment, for example to reproduce an error at your request, security and privacy protections in the non-production environment will be equivalent to those in production.

(b) Pindrop will encrypt your Confidential Information that is subject to long-term storage within Pindrop-Controlled Information Systems and when your Confidential Information is transmitted by Pindrop over public networks. Pindrop will maintain documented procedures for encryption key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use. To the extent that encryption is impractical, Pindrop will use compensating controls designed to protect your Confidential Information.

(c) If Pindrop requires access to your Confidential Information that is stored within Pindrop-Controlled Information Systems, and if the access is managed by Pindrop, Pindrop will deploy measures designed to restrict access to the minimum level required. Such access, including, without limitation, administrative access, will be individual, role-based, and subject to approval and regular validation by authorized Pindrop personnel following the principles of segregation of duties. Pindrop will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke the access upon the account owner's separation or upon the request of authorized Pindrop personnel, such as the account owner's manager.

(d) For Pindrop-Controlled Information Systems, Pindrop will:

(i) monitor and periodically test the Pindrop-Controlled Information Systems to assess the effectiveness of the Security Policy;

(ii) maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and password change frequency;

(iii) monitor use of privileged access and maintain security information and event management measures designed to: (1) identify unauthorized access, use, or tampering; (2) facilitate a timely and appropriate response, and (3) enable internal and independent third-party audits of compliance with the Security Policy;

(iv) where practicable for a given Pindrop-Controlled Information System, use multi-factor authentication designed to protect against unauthorized access to the Pindrop-Controlled Information System;

(v) maintain logs in which privileged access and activity are recorded will be retained in compliance with Pindrop's worldwide records management plan and Security Policy;

(vi) maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of the logs described in (v) above;

(vii) maintain tools designed to detect and remove Malicious Code from the Pindrop-Controlled Information Systems;

(viii) adopt procedures for change management; and

(ix) develop, implement, and maintain procedures for the secure disposal of your Confidential Information within Pindrop's possession or control in any format used in connection with the provision of the Product or Service to the Customer to which it relates, unless the information is necessary for business operations or for other legitimate business purposes or as otherwise expressly authorized by you in this TOS or a Reseller Order, is otherwise required to be retained by law or regulation, as set forth in Section 11(d) (Obligations Upon Termination) in the main body of this TOS, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

(e) Pindrop will securely sanitize physical media intended for reuse prior to the reuse, and will destroy physical media not intended for reuse, consistent with NIST guidelines for media sanitization. Upon your reasonable request, Pindrop will provide a certificate of destruction certifying the destruction of any of Your Confidential Information within Pindrop's possession or control.

8. Service Integrity and Availability Control. With respect to Pindrop-Controlled Information Systems, Pindrop will:

(a) Perform security risk assessments at least annually;

(b) Perform security testing and vulnerability assessments on a periodic basis;

(c) Enlist a qualified testing service to perform penetration testing at least annually;

(d) Perform automated vulnerability scanning against configuration industry standards reasonably designed to identify publicly-known security vulnerabilities in Pindrop-Controlled Information Systems based on Pindrop's risk assessment: (i) at least every six months; (ii) whenever there are material changes to Pindrop's technical operations of the nature that reasonably justify the performance of a scan; and (iii) whenever there are circumstances that Pindrop knows or has reason to know may have a material impact on Pindrop's information security program of the nature that reasonably justify the performance of a scan;

(e) Follow Pindrop's policies with respect to the remediation of identified vulnerabilities, based on associated risk, exploitability, and impact;

(f) Take reasonable steps to avoid disruption of the Products and Services when performing its tests, assessments, scans, and execution of remediation activities;

(g) Maintain measures designed to assess, test, and apply security advisory patches. Upon determining that a security advisory patch is applicable and appropriate, Pindrop will implement the patch pursuant to Pindrop's policies, taking into account associated risk, exploitability, and impact;

(h) Maintain policies and procedures designed to manage risks associated with the application of changes; and

(i) Maintain an inventory of information technology assets.

9. Malicious Code. Pindrop will not intentionally or knowingly either introduce or allow the introduction of any code, files, scripts, agents or programs intended to do harm, including for example, viruses, worms or Trojan horses ("Malicious Code") into the Product delivery environment. If Malicious Code is found to have been introduced into a Product by Pindrop, Pindrop will be responsible for removing the Malicious Code from the Product. If the Malicious Code that was found to have been introduced by Pindrop is also found to have been introduced into Your Information Systems, Pindrop will reasonably cooperate with you by providing relevant information necessary for the you to mitigate the effects of the Malicious Code.

10. Vendor Management Program.

(a) Pindrop agrees to maintain a formal vendor management program. As part of the program, Pindrop is responsible for conducting due diligence on each of its In-Scope Subcontractors on a periodic basis to assess the extent to which each In-Scope Subcontractor has reasonable security measures designed to protect the Your Call Data in that In-Scope Subcontractor's possession or control. In conducting In-Scope Subcontractor due diligence, Pindrop may rely upon the information available in an In-Scope Subcontractor's SOC2 or comparable report or certification (each an "**Independent Audit Report**") to make the assessment, even if the Independent Audit Report does not contain the level of detail specified in this Exhibit C. Upon your request, Pindrop will direct you to the location at which you can obtain copies of an In-Scope Subcontractor's Independent Audit Report. In the event that you are unable to obtain the Independent Audit Report, Pindrop will use reasonable efforts to secure the relevant Independent Audit Report from the In-Scope Subcontractor and provide a copy to you. Pindrop agrees to provide you with a minimum of 30 days' prior notice if there is a material change in the identity of the In-Scope Subcontractors applicable to the Products or Services covered under an existing Reseller Order. If an In-Scope Subcontractor is Processing your Personal Data, then within 30 days of receiving notice of a new In-Scope Subcontractor, you may object (in good faith) to the engagement. If you make a timely objection, the parties will work in good faith to resolve the objection. If the parties are not able to come to a mutually agreed solution, your sole and exclusive remedy is to terminate the relevant Reseller Order under which the new In-Scope Subcontractor is Processing your Personal Data.

(b) In addition to In-Scope Subcontractors, you understand and agree that Pindrop may use other vendor systems and solutions to support its day to day back office business operations where your Confidential Information (other than data that's been input into a Product) may be collected, processed or stored, including by way of example, contract management, billing or other financial transaction-related tools and solutions (each a "**Back Office Business System**"). Back Office Business Systems are not Pindrop-Controlled Information Systems, but are subject to the requirements in Sections 10(c) and 10(d) of this Exhibit C.

(c) Pindrop will have a written agreement in place with each In-Scope Subcontractor and each vendor providing a Back Office Business System that contains commercially reasonable confidentiality obligations designed to protect the confidentiality of Your Call Data in the possession or control of the In-Scope Subcontractor or the confidentiality of your Confidential Information in the possession or control of each vendor providing the Back Office Business System, as applicable.

(d) Pindrop is responsible for any unauthorized disclosure of Your Call Data by an In-Scope Subcontractor and your Confidential Information by each vendor providing a Back Office Business System to the same extent as Pindrop itself would be by the terms of this TOS.

11. BCP Program.

(a) Pindrop's BCP will include (i) a business impact analysis that includes a risk assessment that documents prioritization of business functions and process, systems, subcontractors, resource requirements and interdependencies that may affect recovery timelines and alternative resource plans; (ii) specifically defined or targeted RTOs (recovery time objective); and (iii) specifically defined or targeted RPOs (recovery point objective). Unless provided otherwise in a Reseller Order, Pindrop's RTO and RPO policy for a single availability zone failure for a Product will not exceed 24 hours.

(b) Pindrop will conduct periodic exercises with respect to its BCP (such as tabletop exercises), but on no less than an annual basis. If an event triggers Pindrop's BCP (each a "**BCP Event Trigger**"), Pindrop is responsible for implementing the BCP in accordance with Pindrop's policies and procedures. You understand and agree that if a BCP Event Trigger occurs, depending on the nature and scope of the event and whether you procure "high availability" Appliances for any Products deployed at your managed facilities, the availability and/or ability to recover Your Confidential Information, including without limitation, the Your Call Data, in Pindrop's possession or control may be impacted.

(c) The Products are not designed for and should not be used by you as an official record or similar, whether for regulatory purposes or otherwise.

(d) Should the Products in use by you experience an outage, Pindrop will notify you of the outage and provide periodic status updates until the impact is resolved.

(e) Pindrop will provide reasonable prior notice to you if Pindrop's BCP is changed in a way that would have a material adverse impact in Pindrop's ability to deliver the Products or the Services to you as set forth in the TOS and each Reseller Order.

12. Your Responsibilities. You agree to take commercially reasonable measures designed to detect and prevent the introduction of Malicious Code into Pindrop-Controlled Information Systems used in the delivery of Products or Services to you. You further understand and agree that you are responsible for determining whether the Products and Services are suitable for your use and implementing and managing security measures for all components of the Products and Services that Pindrop does not manage or for which Pindrop does not have security obligations under this Exhibit C, with Pindrop's only security obligations being as set forth in this Exhibit C. Examples of your responsibilities include, without limitation: (a) securing all of Your Information

Systems; and (b) accepting and implementing all security patches provided by Pindrop with respect to any Appliances (and all other software distributed by Pindrop to you in order to enable the security patches), without delay. You agree that Pindrop does not manage, and is not responsible for the security of, Appliances. You further agree that it is your responsibility, and not Pindrop's responsibility, to ensure adequate backups of any of Your Call Data on Your Information Systems that are physically and logically separated from the Products and Services being provided by Pindrop under this TOS. You agree that Pindrop is not in breach of its obligations under this Exhibit C if and to the extent that Pindrop's non-compliance is directly caused by your failure to comply with your own security responsibilities in this TOS.

EXHIBIT D

TTC Appliance Terms

Last Updated: February 3, 2023

These TTC Appliance Terms ("**Appliance Terms**") are incorporated by reference into the End User Terms of Service for Pindrop® Cloud Solutions ("**TOS**"), and describe supplemental or different terms that apply to the Products if the call capture method is Mirror the Call (as defined below), also known as "tap-to-cloud". Capitalized terms not defined in these Appliance Terms are as defined in the TOS, its attached Exhibits, or the Reseller Order. If the TOS and these Appliance Terms conflict, these Appliance Terms control.

1. Definitions.

(a) "**Authorized Site**" means a site located within the Authorized Geography that has been designated in a Reseller Order at which TTC Appliances will be installed and used by you.

(b) "**Manufacturer EULA**" means the manufacturer's standard end user license terms that apply to the Manufacturer Software installed on a TTC Appliance.

(c) "**Manufacturer Services**" means any manufacturer-provided maintenance, support or other professional services related to TTC Appliances and corresponding Manufacturer Software that the manufacturer provides directly to you under a Manufacturer EULA or Other Manufacturer Terms.

(d) "**Manufacturer Software**" means the standard software that is pre-installed (and may be periodically updated) by the manufacturer on a TTC Appliance prior to shipment (i.e., not installed by Pindrop). Manufacturer Software is typically "low level" software or tools used for the basic operation of the TTC Appliance itself.

(e) "**Mirror the Call**" means to mirror the signaling and media for a given call such that the data associated with inbound call to Your Phone Number is concurrently routed to multiple destinations, in this case, (i) Your Call Center Infrastructure for standard handling of that call (i.e., as if the Product were not in use by you); and (ii) the Product for analysis.

(f) "**Other Manufacturer Terms**" means the manufacturer's standard terms that apply to the warranty, support and other services that the manufacturer of a TTC Appliance and its personnel will or may provide directly to you.

(g) "**Pindrop-Provided Software**" means the software, including the Router Software, that Pindrop installs or otherwise provides to you from time to time for installation on the TTC Appliances necessary for the use of the cloud-based portion of the Product. Except as expressly provided otherwise in these Appliance Terms, Pindrop-Provided Software is considered part of the Product. Pindrop-Provided Software does not include Manufacturer Software.

(h) "**Router Software**" means the portion of the Pindrop-Provided Software, including its Third-Party Software Components, that provides the core functionality to Mirror the Call and route the call to a Product for analysis.

(i) "**TTC Appliances**" means hardware purchased from Pindrop (e.g., server, computers, switches, etc.), together with any related materials (e.g., power cords or other similar accessories) for use with a Product covered under these Appliance Terms.

2. Terms of Use.

(a) **Use Requirements.** During each relevant Reseller Order, the TTC Appliances must be dedicated and used solely with the relevant Pindrop-Provided Software and the Product under the relevant Reseller Order for which those TTC Appliances were purchased.

(b) **Pindrop-Provided Software Terms**. During a Reseller Order, you agree to have and maintain (i) the configuration for Your Call Center Infrastructure to collect and transmit the minimum data elements required for the Product to analyze each Call (as detailed in the applicable Order and/or Documentation) and (ii) consistent WAN connectivity (both inbound and outbound). The Router Software and the use and what specific components comprise any other Pindrop-Provided Software are Confidential Information of Pindrop and its licensors. Pindrop-Provided Software contains certain Third-Party Software Components and is subject to the terms and conditions in Section 4(b) (Access to Products and Services) of the TOS. If you violate the terms that apply to Pindrop-Provided Software and fail to timely cure the breach, Pindrop has the right to suspend your access to the Product until you cure the breach or these Appliance Terms are terminated by Pindrop for cause as authorized in the TOS, whichever occurs first.

(c) **Router Software Specific Terms**. The Router Software includes software from 128 Technology, Inc. ("**Licensor**"). Licensor is a third-party beneficiary of the terms that apply to your access, use and installation of its components of the Router Software (but not with respect to any other aspect of the Product or any other rights in these Appliance Terms or the TOS). However, the Licensor is only entitled to exercise those rights if Pindrop and you are unable to resolve the non-compliance amongst themselves within 30 days of the date on which Pindrop has notified you in writing of the non-compliance or such other time period mutually agreed to by the parties. You will not publish or distribute any results of benchmarking test run on the Router Software. Pindrop and its affiliates are authorized to share aggregated network use data (e.g., bandwidth capacity) with the licensors of the Router Software related to the use of the Router Software with the Product so long as neither Pindrop nor its affiliates identify you as the source of the data.

(d) **Additional Terms**.

(i) TTC Appliances, Manufacturer Software installed on the TTC Appliances, and the Manufacturer Services are provided by Pindrop to you on an "as is" basis and without any warranties, support, maintenance, or indemnification (e.g., those rights in Section 10(a) (Infringement Claims Coverage) of the TOS) or other similar rights and benefits of any kind. The Manufacturer EULA and Other

Manufacturer Terms are solely between you and the applicable manufacturer, and Pindrop has no responsibility or liability if the manufacturer breaches those terms. You will look exclusively to the relevant manufacturer for any problems that you experience with TTC Appliances or Manufacturer Software, and for any rights, remedies, or damages if the manufacturer breaches those terms.

(ii) Maintenance and support for TTC Appliances and Manufacturer Software will be provided to you solely by Authorized Reseller or the relevant manufacturer under the terms of the Manufacturer EULA and Other Manufacturer Terms. To the extent an update is issued by the manufacturer for Manufacturer Software, you agree to reasonably cooperate with Pindrop in the testing and installation of any manufacturer update prior to use in a production environment to enable the parties to verify that the update will not create an error in the Product with which the Manufacturer Software and TTC Appliances are being used.

(iii) The recommended usage period for TTC Appliances is 3 years from the relevant Subscription Start Date. However, you are not authorized to use any TTC Appliance that is older than 5 years from the Subscription Start Date of the relevant Product, unless expressly pre-approved otherwise by Pindrop in writing.

3. Term and Termination.

These Appliance Terms are hereby incorporated by reference into the and run concurrently with the TOS. If a given Order is terminated and the subscription for the Product is not renewed, or if a given TTC Appliance is decommissioned, you will provide Pindrop with (A) timely access to each TTC Appliance (no more than 14 days from the effective date of termination or decommissioning, unless the parties agree to an extension in writing); and (B) reasonable cooperation to facilitate secure deletion of all Pindrop-Provided Software and any Pindrop Confidential Information residing on the TTC Appliances. If the parties agree that you will perform the secure deletion, then you will timely notify Pindrop in writing when the secure deletion is completed. You will not retain or otherwise prevent or delay Pindrop from obtaining access to or enabling Pindrop to transfer or remove any files in your possession or control at the time of termination. Failure to do so is a material breach of this TOS. In addition to this Section 3 and any rights that state they survive termination in these Appliance Terms, Sections 2(c) (Router Software Specific Terms) and 2(d) (Additional Terms) survive any expiration or termination of these Appliance Terms.