ACCEPTABLE USE POLICY

Last Updated: April 1, 2026

1. Scope and Applicability

This Acceptable Use Policy ("AUP") applies to Arch Technologies, LLC, (collectively, "Arch Technologies"). This AUP governs each customer of Arch Technologies (each, a "Customer"). Customer shall be responsible for any breach or violation of this AUP by its users, including any individual or entity that accesses or uses the Services through the Customer.

2. Acceptance and Purpose

A. This AUP is established to govern the reasonable and responsible use of Arch Technologies' products and services (collectively, the "Services") by Customers who purchase or use the Services. By accessing or using the Services, Customer shall be deemed to have agreed to be bound by the terms and conditions of this AUP, which is hereby incorporated into all agreements executed by Customer for the procurement of Arch Technologies Services, including any applicable online terms and conditions.

B. The purpose of this AUP is to protect the integrity, security, and reliability of the network; safeguard the interests of Arch Technologies, its Customers, and third parties; and prevent activities that may expose Arch Technologies or its Customers, users, or third parties to legal, regulatory, or operational risk. By establishing clear guidelines for permitted and prohibited uses, this AUP enables Arch Technologies to provide a high standard of Services and to take appropriate action in response to misuse, abuse, or other harmful activity.

3. Violations of this AUP

A. Customer shall be deemed in violation of this AUP if Arch Technologies determines, in its sole discretion, that any action by such Customer or its users in connection with the use of the Services: (a) is inconsistent with the purposes of such Services; or (b) violates any applicable local, state, federal, or international law, statute, regulation, ordinance, executive order, agency decision, or other legally binding governmental directive, including, without limitation, the CAN-SPAM Act of 2003, the Computer Fraud and Abuse Act (18 U.S.C. § 1030 et seq.), the Telephone Consumer Protection Act (47 U.S.C. § 227), the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101–6108), the Federal Trade Commission's Telemarketing Sales Rule, the Digital Millennium Copyright Act, and any applicable Federal Communications Commission ("FCC") rules and orders (collectively, "Applicable Laws").

B. Customer shall also be deemed in violation of this AUP if Arch Technologies determines, in its sole discretion, that any action by such Customer or its users, whether or not in connection

with the use of the Services, has resulted in: (i) harm to Arch Technologies, its reputation, Services, or users; (ii) any third-party blacklisting, blocking, filtering, or refusal of communications originating from or directed to Arch Technologies or its users; or (iii) interference with the transmission of communications over or through the Services.

4. Prohibited Actions

Customer shall use the Services only in a manner that, in Arch Technologies' sole discretion, is consistent with the purposes of such Services. Customer shall not engage in any activity that results in harm to Arch Technologies, the Services, or any user, or that interferes with Arch Technologies' provision of, or any user's use or enjoyment of, the Services.

Customer shall not, and shall not permit any third party to, modify, copy, create derivative works from, reverse engineer, decompile, recompile, disassemble, hack, access without authorization, or otherwise interfere with the Services or any Arch Technologies software or hardware used in connection with the provision of the Services, in whole or in part.

5. Intellectual Property and Proprietary Rights

Customer shall not use the Arch Technologies network or Services to store, transmit, distribute, or make available any content that infringes, misappropriates, or otherwise violates the intellectual property or proprietary rights of Arch Technologies or any third party, including, without limitation, copyrights, trademarks, patents, trade secrets, and rights of privacy or publicity.

Customer is also prohibited from using the Arch Technologies network or Services in any manner that dilutes, infringes, or improperly exploits the intellectual property rights of Arch Technologies.

Customer shall not register, use, or reference any domain name, trademark, or service mark in connection with the Services that is misleading, confusingly similar to, or otherwise violates the rights of Arch Technologies or any third party.

6. Account Security and Password Protection

A. Customer shall be responsible for maintaining the confidentiality and security of all account credentials, including usernames, passwords, authentication keys, and any other access controls used in connection with the Services. Customer shall implement and maintain reasonable administrative, technical, and physical safeguards to prevent unauthorized access to or use of the Services, including, without limitation, the use of strong passwords, periodic credential updates, multi-factor authentication where available, and appropriate access controls.

B. Customer shall not share credentials except as necessary for authorized use of the Services and shall ensure that all authorized users comply with applicable security requirements. Customer shall be fully responsible for all activities conducted through its accounts, whether authorized or unauthorized, except to the extent caused solely by Arch Technologies. Customer shall promptly notify Arch Technologies of any actual or suspected unauthorized access, credential compromise, fraud, or security incident involving the Services and shall cooperate with Arch Technologies in any investigation or mitigation efforts.

C. Customer shall not, and shall not permit any third party to, access or attempt to access any systems, networks, accounts, or data without authorization, or engage in any activity designed to probe, scan, test, or breach the security of the Services or any related systems or networks. Customer shall not circumvent, disable, or otherwise interfere with any security, authentication, or access control measures implemented by Arch Technologies or any third party.

7. Voice Services

The following additional restrictions apply to Voice Services, which are intended primarily for live, two-way communications between individuals.

A. Customer shall not use the Services in any manner that violates Applicable Laws or that is threatening, obscene, defamatory, harassing, deceptive, libelous, fraudulent, malicious, infringing, or invasive of the privacy rights of any individual.

B. Customer shall use the Voice Services only in compliance with Applicable Laws, including those relating to telemarketing, robocalling, call recording, privacy, consumer protection, synthetic or artificial intelligence generated voices, and caller identification.

C. Customer shall not use, or permit any third party to use, the Voice Services for any unlawful, abusive, deceptive, fraudulent, or misleading purpose, including, without limitation, spam calls, scam calls, phishing calls, unsolicited prerecorded messages, or autodialed calls made without required consent.

D. Customer shall not originate, facilitate, or transmit artificial, fraudulent, or manipulated traffic, including traffic pumping, access stimulation, looping traffic, fraudulent answer supervision, false answer or call completion schemes, or any other traffic pattern designed to generate improper compensation or avoid applicable charges.

E. Customer shall not transmit misleading, inaccurate, or unauthorized caller identification information or otherwise violate caller ID authentication requirements, including applicable STIR/SHAKEN obligations.

F. Customer shall implement and maintain safeguards to prevent unauthorized use, toll fraud, spoofing, phishing, PBX hacking, and other forms of voice-related fraud.

G. Customer shall not interfere with, disrupt, degrade, or improperly burden the network or Services.

H. Customer shall not use the Voice Services for continuous playback, call blasting, unlawful mass calling, or other high-volume automated activities not expressly authorized in writing by Arch Technologies.

I. Customer shall not use any numbering resources, including, without limitation, direct inward dial ("DID") numbers, toll-free numbers (including 8YY numbers), automatic number identification ("ANI"), or any other telephone numbers or identifiers associated with the Services, in any manner that is fraudulent, misleading, deceptive, unlawful, or intended to circumvent or evade applicable routing, rating, geographic, compensation,

intercarrier, or billing restrictions. Without limiting the foregoing, Customer shall not: (i) engage in or facilitate traffic pumping, access stimulation, or any scheme designed to artificially inflate call volumes or generate improper intercarrier compensation; (ii) manipulate ANI, caller ID, or numbering information to disguise, misrepresent, or falsify the origin, destination, or identity of traffic; (iii) route traffic in a manner intended to obtain preferential or unauthorized compensation, rates, or routing treatment; (iv) generate artificial, non-bona fide, or looped traffic, including short-duration or high-volume calling patterns designed to exploit billing systems; (v) misuse toll-free numbers or other numbering resources to evade charges, shift costs, or create the appearance of legitimate inbound or outbound communications; or (vi) otherwise exploit numbering resources or the Services for financial gain in a manner inconsistent with their intended purpose.

J. Customer shall implement and maintain reasonable know-your-customer ("KYC") policies, procedures, and controls sufficient to verify the identity of its customers, downstream users, and any other persons or entities authorized to access or use the Services through Customer. Customer shall collect, maintain, and, upon reasonable request, provide accurate and up-to-date information regarding such parties, including information necessary to confirm identity, business purpose, authorized use case, and compliance with applicable law. Customer shall not permit any customer, downstream user, or other third party to access or use the Services unless and until Customer has completed such diligence as is reasonably necessary to assess and mitigate the risks of fraud, unlawful traffic, spoofing, robocalling, or other misuse of the Services. Customer shall maintain records of KYC diligence and shall update such records as necessary to ensure continued accuracy and compliance.

K. Customer shall comply with all applicable robocall mitigation and regulatory requirements, including, without limitation, registration in and ongoing compliance with the Federal Communications Commission's Robocall Mitigation Database ("RMD"), certification of its mitigation program, and implementation of effective measures to prevent the origination or transmission of illegal or unlawful robocalls including but not limited to utilizing analytics systems to monitor traffic for anomalies, handling complaints regarding robocalls, and blocking suspicious traffic. Customer shall maintain accurate and current filings, provide any required certifications, and promptly update such information as necessary to remain in compliance. Customer shall not originate, route, or permit the transmission of traffic that does not comply with such requirements and shall promptly respond to any regulatory inquiries, enforcement actions, or industry traceback requests related to its traffic.

L. Customer shall comply with all applicable caller identification and authentication requirements, including, without limitation, implementation and proper use of STIR/SHAKEN frameworks or any successor or equivalent caller ID authentication regime. Customer shall ensure that all calls originated or transmitted using the Services include accurate and non-misleading caller identification information and shall not engage in or permit any form of caller ID spoofing, manipulation, or misrepresentation of the originating party, except as expressly permitted by applicable law. Customer will restrict A-level attestation to those numbers where it has a direct customer relationship, can verify the identity of the caller, and confirm the use of the number is authorized. Customer agrees

to cooperation in any traceback requests regarding attestation issues and provide documentation of attestation records.

M. Customer shall maintain complete, accurate, and unaltered call detail records ("CDRs") and related records for all traffic originated, transmitted, or received using the Services. Customer shall not modify, falsify, obscure, or misrepresent any such records and shall retain such records for a period consistent with applicable law and industry standards. Upon reasonable request, Customer shall promptly provide such records to Arch Technologies for purposes of fraud investigation, dispute resolution, regulatory compliance, or traceback requests.

N. Customer shall promptly and fully cooperate with any traceback request, regulatory inquiry, or law enforcement request relating to traffic originated, transmitted, or received using the Services. Without limiting the foregoing, Customer shall respond to any traceback request within twenty-four (24) hours of receipt, or such shorter timeframe as may be required by applicable law, regulation, or industry standard, and shall provide complete and accurate information sufficient to identify the source of the relevant traffic.

O. Customer shall comply with all state and federal law regarding call recording including providing proper disclosure, obtaining proper consent, and maintaining consent audit information. Further, Customer is responsible for all jurisdictional compliance regarding call recording.

8. Arch Technologies Remedies

A. Arch Technologies may, in its sole discretion, suspend, restrict, or terminate the Services if it reasonably believes that a violation of this AUP has occurred or is likely to occur. Such action may be taken immediately and without prior notice where required by law, necessary to prevent harm, or to protect Arch Technologies, the network, its customers, or third parties. Arch Technologies may also block specific traffic, numbers, routes, or campaigns as it deems necessary.

B. 4Arch Technologies may cooperate with law enforcement authorities, regulators, and third parties in the investigation of any suspected violation of this AUP, including the disclosure of relevant information. Arch Technologies shall not be liable for any damages arising from actions taken in accordance with this AUP.

C. Failure by Arch Technologies to enforce any provision of this AUP shall not constitute a waiver of its right to enforce such provision or any other provision in the future.

D. Arch Technologies reserves the right to implement technical controls, monitoring mechanisms, and protective measures to prevent violations of this AUP and to collect service-related data in the normal course of business for operational and compliance purposes.

E. Customer shall promptly investigate any complaints, designate a responsible contact for AUP matters, and take all necessary corrective actions to remedy any violation.

9. Arch TechnologiesAudit Right

Customer shall, upon reasonable notice, provide Arch Technologies with access to such records, systems, and personnel as reasonably necessary to verify Customer's compliance with this

AUP in connection with its use of the Services, and shall promptly address and remediate any deficiencies identified by Arch Technologies.

10. Legal and Commercial Protections

A. Customer shall be solely responsible for its use of the Services and for any use by its users, customers, agents, contractors, or other third parties accessing or using the Services through Customer.

B. Customer shall defend, indemnify, and hold harmless Arch Technologiesand its affiliates, officers, directors, employees, and agents from and against any and all claims, demands, damages, losses, liabilities, fines, penalties, costs, and expenses (including reasonable attorneys' fees) arising out of or related to: (a) Customer's or its users' use of the Services; (b) any violation of this AUP or Applicable Laws; (c) any content transmitted, stored, or processed through the Services; or (d) any infringement or misappropriation of any third-party rights.

C. Customer acknowledges that Arch Technologies does not control or monitor all content or communications transmitted through the Services. Except as expressly set forth in an applicable Service Agreement, the Services are provided on an "as is" and "as available" basis, and Arch Technologies disclaims all warranties, whether express, implied, statutory, or otherwise, including, without limitation, warranties of merchantability, fitness for a particular purpose, non-infringement, or uninterrupted or error-free operation.

D. Customer shall comply with all applicable export control, trade sanctions, and similar laws and regulations, including those administered by the U.S. Department of Commerce, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), and any other applicable governmental authority. Customer shall not use, export, re-export, or otherwise make available the Services in violation of such laws or regulations.

E. IN NO EVENT SHALL ARCH TECHNOLOGIES BE LIABLE TO ANY CUSTOMER, USER, OR THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING OUT OF OR RELATED TO THIS AUP OR ANY ACTION TAKEN OR NOT TAKEN UNDER THIS AUP, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, OR OTHER ECONOMIC LOSS, EVEN IF ARCH TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11. AUP Modification

Arch Technologies reserves the right to amend this AUP at any time. Customer is responsible for reviewing this AUP periodically for updates. In the event of any material changes, Arch Technologies may provide notice by email, invoice insert, mail, or any other reasonable means as determined in its sole discretion.

12. Reporting Violations and Inquiries

Customer shall promptly report any known or suspected violations of this AUP, security incidents, fraud, or misuse of the Services to Arch Technologies. Any questions regarding this AUP or reports of violations may be directed to Arch Technologies at support@ringcent.com.