Podium Acceptable Use Policy

This Acceptable Use Policy (the "Policy") sets out rules applicable to your use of the Podium Corporation, Inc. ("Podium", "we", "us" or "our") Services and Podium Technology, including via our clients' websites or platforms (the "Services"). The examples described in this Policy are not exhaustive.

This Policy should be read in conjunction with the Podium Terms of Service ("Podium Terms of Service") (currently available at: https://legal.podium.com/#termsofservice-us) into which it is incorporated by reference. We may suspend, terminate, or take other interim action regarding your access to or use of the Services, if, in our sole judgment, we believe you, directly or indirectly, violated this Policy or authorize or help others to do so.

We may modify this Policy from time to time by posting a revised version on our Website. By using the Services, you agree to the latest version of this Policy. Any capitalized terms not defined in this Policy have the meaning set forth in the Podium Terms of Service.

General Policies/Requirements. We all expect that the messages and communications we want to send and receive will reach the intended recipient(s), unhindered by filtering or other blockers. An important step you can take to make that expectation a reality is to prevent unwanted communications by only sending messages and communications that comply with applicable laws and communications-industry guidelines/standards. To that end, all communications originating from your use of the Podium Services and Podium Technology (including but not limited to SMS, MMS, webchat, Voice, and similar messaging channels available through the Services) are subject to, and must comply with, the Podium Terms of Service, including this Policy, which sets out certain rules and/or prohibitions regarding: Consent ("opt-in"); Revocation of Consent ("opt-out"); Sender identification; Messaging Usage; Prohibited Content; Filtering Evasion; and Enforcement.

- **Consent Requirements**
    - *Standard Consent Requirements.* Prior to sending the first message to an individual, you must obtain agreement from the message recipient to communicate with them - this is referred to as "consent." You must make clear to the individual they are agreeing to receive messages of the type you're going to send.
        - You need to keep a record of the consent, such as a copy of the document or form that the message recipient signed, or a timestamp of when the customer completed a sign-up flow or otherwise provided consent. This record of consent must be retained as set forth by local regulations or best practices after the end user opts out of receiving messages.
        - If you do not send an initial message to that individual within a reasonable period after receiving consent (or as set forth by local regulations or best practices), then you will need to reconfirm consent in the first message you send to that recipient.
        - The consent applies only to you, and to the specific use that the recipient has consented to. Consent can't be bought, sold, or exchanged. For example, you can't obtain the consent of message recipients by purchasing a phone list from another party. You also can't treat it as blanket consent allowing you to send messages from other brands or companies you may have, or additional messages about other uses for which you haven't received consent.
    - *Alternative Consent Requirements.* While consent is always required and the consent requirements noted above are generally the safest path, there are two scenarios where consent can be received differently.
        - *Contact initiated by an individual*
            - If an individual sends a message to you, you may respond in an exchange with that individual. For

example, if an individual texts your phone number asking for your hours of operation, you can respond directly to that individual, relaying your open hours. In such a case, the individual's inbound message to you constitutes both consent and proof of consent. Remember that the consent is limited only to that particular conversation. Unless you obtain additional consent, don't send messages that are outside that conversation.

        - *Informational content to an individual based on a prior relationship*
            - You may send a message to an individual where you have a prior relationship, provided that individual provided their phone number to you, and has taken some action to trigger the potential communication, and has not opted out or otherwise expressed a preference to not receive messages from you.
            - Actions can include a button press, alert setup, appointments, or order placements. Examples of acceptable messages in these scenarios include appointment reminders, receipts, one-time passwords, order/shipping/reservation confirmations, drivers coordinating pick-up locations with riders, and repair persons confirming service call times. The message can't attempt to promote a product, convince someone to buy something, or advocate for a social cause.
    - *Periodic Messages and Ongoing Consent.*
        - If you intend to send messages to a recipient on an ongoing basis, you should confirm the recipient's consent by offering them a clear reminder of how to unsubscribe from those messages using standard opt-out language (defined below). You must also respect the message recipient's preferences in terms of frequency of contact. You also need to proactively ask individuals to reconfirm their consent as set forth by local regulations and best practices.
- **Identifying Yourself as the Sender**
    - Every message you send must clearly identify you (the party that obtained the opt-in from the recipient) as the sender, except in follow-up messages of an ongoing conversation.
- **Opt-out**
    - The initial message that you send to an individual needs to include the following language: "Reply END to unsubscribe," or the equivalent using another standard opt-out keyword, such as STOP, STOPALL, UNSUBSCRIBE,, and QUIT.
    - Individuals must have the ability to revoke consent at any time by replying with a standard opt-out keyword. When an individual opts out, you may deliver one final message to confirm that the opt-out has been processed, but any subsequent messages are not allowed. An individual must once again provide consent before you can send any additional messages.

Prohibited Content. You agree that you will not use the Services, or encourage, promote, facilitate, or instruct others to use the Services, to send messages that contain, offer, promote, reference, or link to any information or content related to any of the following:

- *Solicitations or Advertising.* Any messages, communication, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements or otherwise, that are unsolicited or for which you do not have the proper consent from the intended recipient. If you are a Customer of any Podium Client, this includes using the Services to send any such message, communication, or announcement to a Podium Client or any other person or entity.
- *Illegal, Harmful, or Fraudulent Activities.* Any activities that are illegal, that violate the rights of others, or that may be harmful to others, our operations, or reputation, including but not limited to offering, promoting, disseminating, or facilitating:
    - child pornography, child sexual abuse material, or other sexually exploitative content; fraudulent goods, services, schemes, or promotions;
    - make-money-fast or "get-rich-quick" schemes (including work-from-home programs, risk investment opportunities, ponzi and pyramid schemes);

    - high-risk financial services (including payday loans, short-term high-interest loans, third-party auto or mortgage loans, student loans, or cryptocurrency);
    - third-party lead generation services (such as companies that buy, sell, or share consumer information);
    - debt collection or forgiveness services (including third-party debt collection, debt consolidation, debt reduction, or credit repair programs)
    - illegal or regulated substances (including, but not limited to, Cannabis, CBD, or offers for (or payment transactions relating to) Prescription Drugs that cannot be sold over-the-counter);
    - Gambling;
    - "SHAFT" use cases (Sex, Hate, Alcohol, Firearms, Tobacco, including vaping-related activities);
    - phishing or pharming.
- *Infringing Content.* Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- *Offensive Content.* Content that is harassing, defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable.
- *Harmful Content.* Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, or otherwise effect a security breach, including viruses, Trojan horses, worms, time bombs, or cancelbots.
- *Evasive Content.* Content that is designed to intentionally evade filters, detection, or monitoring (see below)
- *Prohibited Industries.* If you are using Podium's Payment Services, you may not use the services in conjunction with any activities identified as Prohibited Industries, as defined in Podium's Payment Service Terms.

Message Abuse; Falsification of Identity or Origin. You will not send messages using spam bots or other similar systems, alter or obscure mail headers, provide false identification, or assume a sender's identity without the sender's explicit permission. You will also not create a false identity or attempt to mislead others as to the identity of the sender or the origin of any data or communications.

Evasion. You may not use the Services or Podium Technology to evade Podium's (including our subcontractor's) or a telecommunications provider's unwanted messaging detection and prevention mechanisms. Examples of prohibited practices include:

- Content designed to evade detection. As noted above, we do not allow content which has been specifically designed to evade detection by unwanted messaging detection and prevention mechanisms. This includes intentionally misspelled words or non-standard opt-out phrases which have been specifically created with the intent to evade these mechanisms.
- Snowshoeing. We do not permit snowshoeing, which is defined as spreading similar or identical messages across many phone numbers with the intent or effect of evading unwanted messaging detection and prevention mechanisms.
- Use of shared public URL shorteners. Where a web address (i.e., Uniform Resource Locator (URL)) shortener is used, you should not use links that have been shortened using shared public URL shorteners like Bitly or TinyURL. If you want to include shortened URLs in your messages, we recommend using a dedicated short domain.

Reverse Engineering and Related Restrictions. You will not (a) modify or create a derivative work of the Services or any portion thereof; (b) reverse engineer, disassemble, decompile, translate, or otherwise seek to obtain or derive the source code, underlying ideas, algorithms, file formats, or non-public APIs to any Services, except to the extent expressly permitted by applicable law and then only upon advance notice to Podium; (c) break or circumvent any security measures or rate limits for the Services; or (d) remove or obscure any proprietary or other notices contained in the Services, including in any reports or output obtained from the Services.

Scope of Use and Reasonable Use Limits. Unless otherwise specified in your applicable Subscription Documentation, all Services (including, in particular, Bulk Messages, Automations, bulk uploads, and/or the Podium API) are subject to the Scope of Use limits listed at https://www.podium.com/pricing/. Additionally, any Services for which specific Scope of Use limits have not been expressly designated, or which have been designated as "unlimited", are intended (and may only be used) for normal business use in compliance

with the Agreement, including this AUP and your Subscription Documentation. Any unusually high or excessive usage of the Services, or use of the Services beyond any applicable Scope of Use limit(s), may impair Podium's ability to provide the Services to you and other Podium users, in which case Podium may suspend or terminate your use of and/or access to the Services. Other use restrictions, applicable to specific Podium Services, may also be found in the Additional Terms applicable to those Services.

Our Monitoring and Enforcement. We reserve the right, but do not assume the obligation, to monitor content on and sent through the Services and to investigate any violation of the Podium Terms of Service, including this Policy, or misuse of the Services. We may remove or disable access to any user, content, or resource that violates the Podium Terms of Service or this Policy or any other agreement we have with you for use of the Services. We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We may also cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

Reporting Violations. If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation.