SMACKDAB INC. OFFICIAL POLICY

ACCEPTABLE USE POLICY

Official legal PDF. This document is generated from the Smackdab website legal source file.

SMACKDAB INC. ACCEPTABLE USE POLICY (AUP)

Effective Date: April 26, 2025

Last Updated: November 1, 2025

Version:

2.1 **TABLE OF CONTENTS**

1. INTRODUCTION AND SCOPE

This Acceptable Use Policy ("AUP" or "Policy") governs the use of all software, services, platforms, websites, applications, APIs, and related offerings provided by Smackdab Inc. ("Smackdab," "we," "us," or "our"), including but not limited to the Smackdab CRM platform, mobile applications, and add-on services (collectively, the "Services").

This Policy applies to all clients, customers, users, and their authorized representatives or end-users (collectively, "You" or "Your") who access or use the Services, regardless of location, jurisdiction, or method of access.

It is designed to prevent misuse or abuse of the Services, protect Smackdab's network, services, and customers, and ensure compliance with applicable laws and regulations.

This AUP is incorporated by reference into the Smackdab Inc.

Terms of Service ("TOS") available at https://smackdab.ai/legal/terms-of-service.

Authorized Users must be 18+ (or the age of majority in their jurisdiction if higher) to use the Services, as set forth in the TOS.

By accessing or using the Services, You acknowledge that You have read this Policy and agree to comply with its terms.

If You do not agree with any aspect of this Policy, You must immediately discontinue use of the Services.

**You are solely responsible for your compliance and the compliance of your authorized users and end-users with this AUP.

Violation of this Policy constitutes a material breach of the TOS and may result in immediate suspension or termination of Your access to the Services, without prior notice.**

2. DEFINITIONS

For purposes of this Policy, the following terms shall have the meanings ascribed to them below:

"Applicable Law" means all federal, state, local, and international laws, statutes, regulations, ordinances, rules, codes, edicts, decrees, judgments, injunctions, orders, and other legally binding requirements applicable to Your use of the Services, including but not limited to laws relating to privacy, data protection, intellectual property, consumer protection, telecommunications, export control, national security, and criminal activity.

"Content" means all text, data, information, software, graphics, messages, tags, interactive features, or any other materials that You may view on, access through, or contribute to the Services.

"High-Risk Activities" means uses where failure of the Services could lead to death, personal injury, or severe environmental or property damage (e.g., medical devices, air traffic control, autonomous vehicles, nuclear facilities).

**"Malicious

Code"** means viruses, worms, time bombs, Trojan horses, malware, spyware, ransomware, adware, keyloggers, rootkits, backdoors, or any other harmful or malicious code, files, scripts, agents, or programs designed to interfere with, damage, disrupt, disable, overburden, impair, or limit the functionality of any computer software, hardware, network, telecommunications equipment, or other device or system.

"Payment Network Rules" means the written rules, regulations, standards, releases, interpretations, and other requirements imposed or adopted by payment card networks (e.g., Visa, MasterCard, American Express, Discover) or other payment systems (e.g., ACH, wire transfer networks).

"Personal Data" means any information relating to an identified or identifiable natural person as defined under applicable privacy laws.

"Sensitive Data" means special categories of Personal Data as defined under applicable privacy laws, including data revealing racial or ethnic origin, political

opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation, or data relating to criminal convictions and offenses.

3. POLICY UPDATES

Smackdab reserves the right to modify this AUP at any time by posting a revised version on our website at https://smackdab.ai/legal/acceptable-use-policy or by providing other notice as specified in the TOS.

Modifications are effective upon posting or as otherwise stated in the notice.

For material changes to this Policy, Smackdab will provide at least 30 days' advance written notice via email to the email address associated with Your account.

For changes required by law or to address an urgent security issue, shorter notice may apply.

Your continued use of the Services after the effective date specified in the notice constitutes your acceptance of the revised AUP.

No reduction of protection during an active term. During an active subscription term, Smackdab will not make changes to this AUP that materially reduce security or privacy protections, except where required by law or to address an urgent security issue (see TOS Section 15.16).

It is your responsibility to review this AUP periodically.

The "Last Updated" date at the top of this Policy indicates when it was last revised.

If you do not agree with any amendments, you must immediately discontinue your use of the Services.

---

4. PROHIBITED CONDUCT AND CONTENT

You may not use the Services, nor permit others to use the Services, to engage in, promote, facilitate, or host any of the following activities or content. The following list is not exhaustive, and Smackdab reserves the right to determine, in its sole discretion, whether any use constitutes a violation of this Policy or its spirit.

4.1. Illegal and Harmful Activities

- Engaging in any activity that is illegal under applicable local, state, federal, or international law or regulation, including but not limited to laws relating to computer crimes, privacy, intellectual property, data protection, identity theft, fraud, stalking, defamation, harassment, or child protection.
- Transmitting, storing, displaying, distributing, or otherwise making available material that violates any applicable law, including criminal laws, or infringes upon or misappropriates the rights of any third party (including intellectual property, privacy, publicity, or contractual rights).
- Promoting or facilitating violence, terrorism, or related activities; providing instructions on creating or using weapons, explosives, or other harmful devices or substances.
- Engaging in activities that are deceptive, fraudulent, inaccurate, or misleading, including social engineering, phishing, or impersonation.
- Displaying or promoting hate speech, harassment, abusive content, or material advocating discrimination against individuals or groups based on race, ethnicity, religion, gender, gender identity or expression, sexual orientation, disability, age, national origin, veteran status, or other protected characteristics under applicable law.
- Displaying material that exploits children under 18 years of age, depicts child abuse, or violates child protection laws, including but not limited to the Children's Online Privacy Protection Act (COPPA).
- Engaging in libelous, defamatory, scandalous, threatening, or excessively profane activity.

4.2. Offensive and Inappropriate Content

- Transmitting, storing, displaying, distributing, or otherwise making available obscene, indecent, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable material.
- Providing, selling, or offering pornography, illicitly pornographic sexual products, escort services, or adult "swinger" material.
- Creating, displaying, storing, or transmitting Content that is grossly offensive, insensitive, upsetting, intended to disgust, or in exceptionally poor taste, particularly Content that promotes, encourages, or depicts extreme acts of violence or cruelty.

4.3. Security Violations and Network Abuse

- Uploading, transmitting, or distributing Malicious Code or creating or using any program, device, or script with the intent to interfere with the proper functioning of the Services or any system, server, or network connected to the Services.
- Attempting to gain unauthorized access to any system, network, service, or account ("hacking"), including any attempt to probe, scan, or test the vulnerability of a system or network, or to breach security or authentication measures without proper authorization.
- Engaging in denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, or any activity that interferes with or disrupts the integrity, performance, or availability of the Services or networks connected to them.
- Performing network scanning, vulnerability scanning, penetration testing, or load testing **without prior written authorization from Smackdab**; provided, however, that security research conducted **in compliance with Smackdab’s Responsible Disclosure Policy (VDP)** is permitted.
- Engaging in illegal peer-to-peer file sharing or unauthorized sharing of copyrighted material.
- Circumventing or attempting to circumvent any security measures or usage restrictions implemented by Smackdab, including by disguising or masking your identity or network traffic.
- Compromising the security or operation of Smackdab systems or the Services through unauthorized access, privilege escalation, or similar actions.
- Using or attempting to use any automated means (including but not limited to bots, scrapers, or other automated tools) to access the Services or to extract data from the Services, except as expressly permitted by Smackdab through an authorized API.

4.4. Intellectual Property Violations

- Using the Services in a manner that infringes or misappropriates the intellectual property rights (copyrights, trademarks, patents, trade secrets) or proprietary rights of Smackdab or any third party. This

includes distributing software, music, videos, images, or other material without necessary rights or consents.

- Removing, obscuring, or altering any copyright, trademark, patent, or other proprietary rights notices associated with the Services.
- Using Smackdab trademarks, logos, or service marks, or any confusingly similar marks, without Smackdab's prior written consent.
- Reverse engineering, decompiling, disassembling, or attempting to derive the source code of the Services or any component thereof, except as permitted by applicable law.

4.5. Misrepresentation and Deception

- Creating a false identity, impersonating another person or entity (including Smackdab), or otherwise misrepresenting the source or origin of any communication or content, such as by forging headers or other identifying information in connection with emails, posts, or other electronic communications.
- Engaging in phishing, pharming, pretexting, social engineering, or other activities designed to obtain personal information, financial information, or access credentials from others under false pretenses.
- Falsely implying any sponsorship, affiliation with, or endorsement by Smackdab or any third party.
- Engaging in fraudulent activities or misrepresenting Your products, services, or other offerings.

4.6. Unsolicited Communications (Spam) and Messaging Abuse

- Generating or facilitating unsolicited commercial email (spam) in violation of the CAN-SPAM Act, TCPA, or other applicable anti-spam laws.
- Sending email or messages to recipients who have not provided verifiable prior express consent (opt-in) or who have opted out.
- Using purchased, rented, borrowed, or third-party email/phone lists where recipients did not directly consent to receive communications *from You*.
- Failing to include valid contact information (physical address) and a clear, functional opt-out mechanism in commercial emails.
- Using misleading or false headers, from lines, subject lines, sender names, or titles in emails, messages, or posts.
- Sending voice calls (especially automated or pre-recorded) or text messages (SMS/MMS) in violation of the Telephone Consumer Protection Act (TCPA), Telemarketing Sales Rule (TSR), National Do-Not-Call Registry rules, or other applicable telemarketing and consumer protection laws and regulations (refer also to the Smackdab Voice and Messaging Policy at https://smackdab.ai/legal/voice-messaging-policy).

- Violating applicable guidelines published by the CTIA, Mobile Marketing Association, or other relevant industry bodies or carrier requirements.
- Employing deceptive, misleading, or unethical marketing practices.

4.7. Specific Restricted Business Practices and Content

- Sale or promotion of illegal drugs, controlled substances (including marijuana/CBD, even where legal locally), or drug paraphernalia.
- Sale or promotion of prescription drugs (unless fully compliant with all applicable laws and platform policies).
- Firearms, ammunition, explosives, or weapons regulated under applicable law.
- Products or services frequently associated with spam or high complaint rates, such as:
- Online pharmacies (especially those not requiring prescriptions).
- Nutritional, herbal, or vitamin supplements making unsubstantiated claims.
- Weight loss products/programs making unrealistic claims.
- Certain dating services associated with deceptive practices.
- Horoscopes, psychic services, or fortune-telling marketed deceptively.
- Work-at-home schemes, "get rich quick" offers, or business opportunities that promise unrealistic returns.
- Lead generation services that involve selling or renting contact lists without adequate consent.
- Credit repair or debt relief/consolidation offers that violate applicable consumer protection laws.
- Stock picks, day trading tips, or high-risk financial services/investment schemes that may violate securities laws.
- Mortgage offers (subject to specific legal compliance with applicable lending laws).
- Gambling services (including online casinos, sports betting, lotteries) without appropriate licensing.
- Cryptocurrency mining, sales, exchanges, or initial coin offerings (ICOs) that violate applicable securities laws or financial regulations.
- Pyramid schemes, Ponzi schemes, or multi-level marketing (MLM) businesses that violate applicable laws.

- Affiliate marketing focused solely on generating commissions without providing substantial value or making required disclosures.
- Debt collection services not in compliance with the Fair Debt Collection Practices Act (FDCPA) or applicable state law.
- Sale or promotion of counterfeit goods or pirated software/media in violation of trademark or copyright laws.

4.8. API Usage Restrictions

- APIs must be used solely for the purpose of accessing and using the Services as intended and licensed under the TOS, and in accordance with any provided API Documentation.
- You must strictly adhere to any usage limits, rate limits, call restrictions, or other policies related to API use published by Smackdab.
- APIs may not be used to circumvent contractual usage limits, access restrictions, security measures, or license limitations.
- APIs may not be used, directly or indirectly, to develop, enable, or support a product or service that competes with the Smackdab Services.
- You may not misrepresent Your identity or the purpose of Your application when accessing APIs.
- You may not share, sell, or redistribute API keys or access credentials.

4.9. Brand Usage Restrictions

- You may not use Smackdab's trademarks, service marks, logos, trade names, trade dress, or other brand assets ("Smackdab Marks") without prior written permission from Smackdab. Any authorized use must comply with Smackdab's brand usage guidelines.
- You may not use Smackdab Marks in any way that falsely implies endorsement, sponsorship, affiliation, or partnership, or in a manner that disparages or harms Smackdab's reputation or goodwill.
- You may not register domain names, social media accounts, or other online identifiers that incorporate Smackdab Marks or confusingly similar variations.

4.10. Protection of Smackdab Content and Service Integrity

- You may not reproduce, modify, copy, distribute, create derivative works from, publicly display, publicly perform, republish, download, store, or transmit any of Smackdab's proprietary materials forming part of the Service (including text, graphics, images, software, user interface elements, underlying code, data compilations, documentation, etc.), except as explicitly permitted by the license granted in the TOS for Your normal use of the Service.

- You may not use any robot, spider, scraper, or other automated means to access, monitor, or copy any part of the Service or Smackdab's proprietary content or code without prior written permission.
- You may not reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code or underlying structure of the Services (except as permitted by law).
- You may not reformat or frame any portion of the web pages that are part of the Services.
- You may not attempt to probe, test, or evaluate the vulnerability of the Services or any related system or network without express prior written authorization.

---

5. SPECIFIC REQUIREMENTS

5.1. Email Marketing

- All email lists used with the Services must be 100% solicited opt-in lists. You must maintain verifiable proof of consent for all recipients, including the date, time, and method of consent, and specific communications the recipient agreed to receive.
- You must clearly identify yourself as the sender of all email communications and ensure Your subject lines accurately reflect the content of Your message.
- All commercial emails must comply with the CAN-SPAM Act, including:
- A valid physical postal address
- A clear and non-deceptive subject line
- A functional unsubscribe mechanism that is honored promptly (within 10 business days)
- Clear identification that the message is an advertisement
- Truthful routing information (From, To, Reply-To)
- You must maintain current and actionable suppression lists (do-not-email lists) and ensure all opt-out requests are processed within 10 business days.
- Selling, renting, or sharing email lists is prohibited, unless You have explicit permission from the individuals on those lists to share their information for such purposes.
- Your email sending practices must comply with industry standards for delivery (bounce handling, complaint processing, etc.) and maintain spam complaint rates below 0.1% at all times.

5.2. Messaging Compliance

- Use of voice and SMS/MMS features must comply with the Smackdab Voice and Messaging Policy at https://smackdab.ai/legal/voice-messaging-policy.
- You must obtain prior express written consent where required by law before sending marketing messages via phone, SMS, or pre-recorded calls.
- All text messages must contain clear identification of the sender and, for marketing messages, a compliant opt-out mechanism.
- Standard opt-out keywords (such as STOP, CANCEL, UNSUBSCRIBE, QUIT, END, and OPT-OUT) must be honored immediately; only a single confirmation message may be sent.
- You must comply with time-of-day restrictions applicable in the recipient's location.
- You must adhere to frequency limits and content restrictions per carrier requirements and applicable regulations.
- You must immediately honor all Do-Not-Call requests and maintain compliant Do-Not-Call lists.

5.3. Privacy Policy

- You must publish, maintain, and abide by a privacy policy that complies with Applicable Laws (including CCPA, GDPR, and other privacy regulations as applicable) and accurately discloses how You collect, use, and share personal information obtained from Your customers or contacts, including through Your use of the Services.
- Your privacy policy must be at least as protective as the Smackdab Privacy Policy available at https://smackdab.ai/legal/privacy-policy.
- Your privacy policy must be easily accessible to Your users, written in clear and plain language, and must be kept current.
- You may not sell, loan, or pledge personal information of Your customers in violation of Your privacy policy or Applicable Law.
- You must provide legally required mechanisms for individuals to exercise their privacy rights (access, deletion, opt-out of sale, etc.) in accordance with applicable privacy laws.

5.4. Payment and Financial Services

- If You use the Services to process payments or engage in financial activities, You must comply with:
- All applicable financial regulations (including Anti-Money Laundering laws)
- Payment Card Industry Data Security Standard (PCI DSS)
- Payment Network Rules

- The Smackdab Pay Processing Agreement (if applicable) available at https://smackdab.ai/legal/pay-processing-agreement
- You must maintain appropriate security measures to protect payment information and financial data.
- You must provide clear refund policies and terms of service to Your customers before collecting payment.

5.5. Account Security

- You are responsible for maintaining the security of Your account credentials and must not share passwords or access information.
- You must implement strong authentication practices for Your users of the Services, including using multi-factor authentication where available.
- You must promptly notify Smackdab of any known or suspected security breaches involving Your account or data.
- You must ensure Your employees and users receive appropriate training on secure use of the Services.

---

6. MONITORING AND ENFORCEMENT

6.1. Monitoring Rights

- Smackdab reserves the right, but does not assume the obligation, to monitor any activity and content associated with the Services for potential violations of this AUP.
- By using the Services, You expressly acknowledge and consent that Smackdab may:
- Monitor Your account activity and content
- Analyze traffic patterns and usage data
- Inspect or scan content transmitted through the Services for compliance with this Policy
- Investigate suspected violations of this AUP
- Smackdab respects the privacy of Your data and will limit monitoring activities to those reasonably necessary to enforce this Policy and comply with applicable laws.

6.2. Investigation and Evidence

- Smackdab may investigate suspected violations of this AUP through various means, including but not limited to:
- Reviewing Your account activity and content

- Analyzing login and usage patterns
- Examining email, message, or call logs
- Reviewing complaints from third parties
- Requesting additional information from You
- You agree to cooperate with Smackdab's reasonable investigation of suspected violations of this Policy, including by providing information and assistance as requested.
- Smackdab may preserve and store Your content and account information if we believe in good faith that such preservation is necessary to:
- Comply with legal process or request
- Enforce this Policy or the TOS
- Respond to claims of violation of third-party rights
- Protect the rights, property, or safety of Smackdab, its users, or the public

6.3. Consequences

- Violation of this AUP constitutes a material breach of the TOS. Smackdab may, in its sole discretion and without liability to You, take one or more of the following actions:
- Issue warnings (written or verbal)
- Suspend Your access to the Services (or specific features) immediately and without prior notice
- Terminate Your account and access to the Services immediately and without prior notice
- Block or filter content or communications deemed to violate this AUP
- Report illegal activities to appropriate law enforcement or regulatory authorities
- Pursue legal action to recover damages, costs (including attorneys' fees), and seek injunctive relief
- Smackdab's response to violations will be proportionate to the nature and severity of the violation, but Smackdab reserves the right to immediately suspend or terminate Services in cases of serious violations or where necessary to prevent harm or liability.
- The failure of Smackdab to enforce this Policy in every instance does not constitute a waiver of its right to do so.

6.4. Liability

- You are solely responsible for any damages, losses, costs, fines, penalties, or expenses (including reasonable attorneys' fees) incurred by Smackdab or third parties resulting from Your violation of this AUP.
- You agree to indemnify and hold Smackdab harmless as set forth in the TOS Section 9.4 (Indemnification by Customer).
- Smackdab is not responsible for any damages, losses, or liability that You or any user may incur as a result of Smackdab's enforcement of this Policy, including suspension or termination of Services.

---

7. REPORTING VIOLATIONS

If You become aware of any violation of this AUP by anyone using the Services (including Yourself or Your users), You agree to notify Smackdab immediately. Please report suspected violations to:

Email: security@smackdab.ai **Mail:** Smackdab Inc. ATTN: Legal/AUP Compliance 372 Live Oak Ln, Marco Island FL 34145 United States

Please include detailed information about the suspected violation, including:

- The nature of the violation
- When it occurred
- Who was involved
- Any evidence You have of the violation (screenshots, message copies, etc.)
- Any harm or damage that has resulted

Smackdab will review reports and take appropriate action in its discretion. Smackdab may not disclose the specific actions taken in response to a reported violation due to privacy, legal, or security considerations.

False or malicious reports of violations may themselves constitute a violation of this Policy.

---

8. LEGAL PROVISIONS

8.1. Governing Law and Jurisdiction

This AUP shall be governed by and construed in accordance with the laws of the State of Florida, without regard to its conflict of law provisions, as specified in Section 13 of the TOS.

8.2. Dispute Resolution

Any disputes arising from or relating to this AUP shall be resolved according to the Dispute Resolution procedures set forth in Section 14 of the TOS, including the binding arbitration provision and class action

waiver.

8.3. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SMACKDAB BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA, OR OTHER INTANGIBLE LOSSES, ARISING OUT OF OR RELATING TO THIS AUP OR ITS ENFORCEMENT.

8.4. Waiver and Severability

The failure of Smackdab to exercise or enforce any right or provision of this AUP shall not constitute a waiver of such right or provision. If any provision of this AUP is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision, and the other provisions of this AUP remain in full force and effect.

8.5. Assignment

You may not assign or transfer this AUP, by operation of law or otherwise, without Smackdab's prior written consent. Any attempt by You to assign or transfer this AUP without such consent will be null and void. Smackdab may assign or transfer this AUP, at its sole discretion, without restriction.

8.6. Survival

The provisions of this AUP that by their nature should survive termination shall survive termination, including, without limitation, ownership provisions, warranty disclaimers, indemnity, and limitations of liability.

8.7. Entire Agreement

This AUP, together with the TOS and other incorporated policies, constitutes the entire agreement between You and Smackdab concerning Your use of the Services, and supersedes all prior or contemporaneous communications and proposals, whether electronic, oral, or written, between You and Smackdab with respect to the Services.

---

9. CONTACT INFORMATION

If You have questions about this Acceptable Use Policy, please contact us at:

Email: legal@smackdab.ai **Mail:** Smackdab Inc. ATTN: Legal Department 372 Live Oak Ln, Marco Island FL 34145 United States **Phone:** +1 (239) 299-4616

DISCLAIMER

This AUP provides guidelines for acceptable use but does not constitute legal advice. The list of prohibited activities and content is not exhaustive. You are solely responsible for ensuring Your use of the Services

complies with all Applicable Laws and regulations in Your jurisdiction and the jurisdictions of those You interact with. Consultation with qualified legal counsel regarding compliance is recommended.

© 2025 Smackdab Inc. All rights reserved.

This PDF is the formal downloadable version of ACCEPTABLE USE POLICY.