SERVEGUARD

ServeGuard Restaurant Terms of Service

Effective date: October 12, 2026

These ServeGuard Restaurant Terms of Service (the "Terms") are a legally binding agreement between ServeGuard LLC, a Delaware limited liability company ("ServeGuard," "we," "us," or "our"), and the restaurant, caterer, or other food-service business that accepts these Terms or uses the Restaurant Service ("Customer," "you," or "your"). The person accepting these Terms represents that the person is authorized to bind Customer. If that person lacks authority, or Customer does not agree, Customer must not use the Restaurant Service.

These Terms govern the ServeGuard Restaurant mobile application, restaurant administrative tools, Menu QR codes, menu-management and training workflows, and retained legacy records, related websites, support, and associated services (collectively, the "Restaurant Service"). An order form, invoice, subscription confirmation, or separately signed agreement may supplement these Terms (each, an "Order Form"). If an Order Form expressly conflicts with these Terms, the Order Form controls only for that conflict. The Data Processing Addendum ("DPA") controls over these Terms for its subject matter.

Current menu experience

ServeGuard currently provides restaurant menu discovery, guest-controlled allergy and dietary filters, and restaurant menu-management and training tools. Menu QR codes identify a restaurant location, not a table, diner, check, or order. Available menus follow the restaurant’s active-menu and scheduling settings. Selecting filters does not submit an allergy report, notify staff, request a food modification, create a review, or confirm that food is safe.

When you continue to a menu, the web QR page or updated diner app sends the selected filter names to ServeGuard to increment the restaurant location’s aggregate totals: menu opens, opens with allergies, and counts for each allergy or dietary preference. No individual menu response, name, account identifier, table, reservation, or per-visit selection record is saved for these totals. Detailed selections are not shown to restaurant staff. Requests still involve ordinary technical information processed by hosting providers; this is not a promise of completely anonymous browsing. Changing filters after opening the menu does not add another count, and repeat menu entries may count again.

In the updated iOS diner app, optional saved allergy profiles remain account-linked and stored with the existing affirmative storage consent. Detailed menu history and the filters used are stored on the device, separated by signed-in account and excluded from app cloud backup. The detailed history is not uploaded; the separate aggregate-count request described above carries no account authentication token or history record. They do not sync between devices. You can delete a menu visit in History. Completing account deletion on a device also clears its local menu history; local copies on other devices must be removed on those devices or by deleting the app.

Table and event check-ins, staff allergy notifications, new reviews, and table assignments are paused in this experience. Their code and prior records are retained, subject to the existing deletion schedules and rights. References below to submissions, sharing with restaurants, response downloads, and reviews describe earlier records and the retained legacy workflow; they do not mean that choosing menu filters activates those features. Any future restoration requires a new product and privacy review and appropriate notice and consent before new collection or sharing.

1. Eligibility, accounts, and authority

1. Customer must be a restaurant, caterer, or food-service business operating in the United States. Owner and administrator accounts must be used by individuals who are at least 18 years old. Customer may authorize staff members who are at least 16 years old only when lawful, appropriate to their job duties, supervised as required, and consistent with workplace and child-labor laws.
2. Customer must provide accurate account, business, location, billing, and contact information; keep it current; protect credentials and verification methods; and promptly notify ServeGuard of suspected unauthorized access.
3. Customer controls which owners, managers, and staff may access its account and locations. Customer is responsible for their acts and omissions, for promptly removing access when no longer appropriate, and for ensuring that each user receives necessary training and uses the Restaurant Service only for Customer's authorized business purposes.
4. Customer may not share individual credentials, allow an unauthorized person to use an account, bypass access controls, or misrepresent a user's role. ServeGuard may rely on actions taken through properly authenticated Customer accounts.

2. What ServeGuard does—and does not do

1. The Restaurant Service lets Customer publish and maintain menus, provide guests with self-directed menu filters, and manage staff training. Customer must keep menu ingredients, allergen labels, modifications, approval status, and availability accurate and current. Filters are based on that information and do not verify ingredients or assess cross-contact.
2. ServeGuard is not a restaurant operator, food preparer, healthcare provider, emergency service, dietitian, allergist, laboratory, food-safety authority, insurer, certifier, or guarantor. ServeGuard does not diagnose allergies, determine whether food is safe, supervise Customer's personnel, inspect kitchens, validate ingredient or cross-contact claims, or replace direct communication between a diner and Customer.
3. A "verified" designation means only that ServeGuard completed the business or setup checks identified in the Restaurant Service at that time. It is not a medical, safety, legal-compliance, ingredient, cross-contact, or quality certification and must not be represented as one.
4. Customer remains solely responsible for food preparation, ingredient and supplier controls, cross-contact prevention, staff training, kitchen operations, legal compliance, and all communications and decisions concerning whether and how to serve a diner.

3. Customer safety responsibilities

Customer must maintain procedures reasonably designed for allergy and dietary communications, including all of the following where applicable:

- having trained personnel directly confirm the diner's needs before ordering and before service;
- communicating the information to appropriate front-of-house and kitchen personnel;
- checking current ingredients, substitutions, preparation methods, shared equipment, and cross-contact risks;
- declining or modifying service when Customer cannot safely accommodate a request;
- treating ServeGuard notifications and records as supplemental, not as the sole safety control;
- following applicable food-safety, employment, accessibility, consumer-protection, and emergency requirements; and
- contacting emergency services when an emergency may exist. ServeGuard is not monitored as an emergency channel.

Customer must not instruct diners or personnel to rely exclusively on ServeGuard, a QR code, a push notification, a displayed record, or a downloaded document. Customer must not represent that ServeGuard eliminates risk or guarantees an allergen-free meal.

4. Earlier allergy submissions and retained QR workflows

1. A diner submission records what the diner entered or selected. ServeGuard does not rewrite the substance of a submission for Customer, resolve inconsistencies, or determine accuracy. Customer must use the most recent applicable submission and directly confirm it with the diner.
2. Restaurant-facing allergy submissions are designed to remain unchanged after submission so the record reflects what was transmitted. Authorized support may cross-reference a submission to troubleshoot a specific request, but ServeGuard does not decide factual disputes or alter a submission to favor either party.
3. A QR submission session expires five minutes after the form is opened. The diner must rescan after expiration. QR codes and URLs may be replaced, disabled, or reissued for security or operational reasons. Customer must use only QR materials generated for the correct Customer location, table, or event and must promptly remove obsolete codes.
4. Customer must safeguard displayed QR codes from substitution or tampering, periodically inspect physical codes, and report suspected tampering. Customer may not redirect, clone, modify, scrape, or embed ServeGuard QR workflows in an unauthorized service.
5. ServeGuard may provide a temporary, access-controlled download option for the diner's submitted record. That copy is informational and does not replace Customer's direct confirmation or procedures.

5. Data roles, permitted use, and confidentiality (including earlier records)

1. For personal data Customer directs ServeGuard to process through the Restaurant Service, Customer is generally the business, controller, or analogous regulated entity, and ServeGuard is generally Customer's service provider or processor, as further described in the DPA. ServeGuard may act independently for account security, fraud prevention, billing administration, legal compliance, and operation of its own business.
2. Customer may use diner allergy, dietary, identifier, and review information only for the applicable visit or event, safety and service follow-up, authorized support, recordkeeping required by law, and other purposes clearly disclosed to and authorized by the diner. Customer may not use that information for advertising, marketing, profiling, unrelated analytics, employee retaliation, eligibility decisions, sale, data brokerage, or training an artificial-intelligence model.
3. Customer must limit access to owners, authorized managers, and personnel who need the information for their duties. Customer must maintain confidentiality, use reasonable safeguards, and avoid copying sensitive data into personal email, consumer messaging apps, unsecured notes, or unrelated systems.
4. Customer must not enter diagnoses, complete medical records, government identifiers, payment-card data, or other unnecessary sensitive information into free-text fields. If Customer receives such information, it must minimize and protect it according to applicable law.
5. Diner identifiers and restaurant-facing allergy-response records are stored separately within the Restaurant Service. Restaurant-facing allergy records are scheduled for automatic deletion 90 days after submission, unless deleted earlier or temporarily preserved when legally required. Customer must not attempt to defeat this retention control.
6. Restaurant-facing reviews may be viewed only by owners and authorized managers. A review includes the diner's chosen display name; one-to-five ratings for Service, Food, Allergy Communication, and Atmosphere; and a calculated overall average, but does not include written comments or the diner's account email. Customer may use reviews for service, safety, and quality improvement, but not to contact or market to a diner unless the diner separately asked to be contacted. Public aggregate ratings are displayed only when ServeGuard's minimum publication threshold is met, which is currently five eligible reviews.

6. Customer content and menu imports

1. "Customer Content" means information, menus, photos, branding, location details, training materials, and other content Customer provides. Customer retains ownership of Customer Content and grants ServeGuard a nonexclusive, worldwide, royalty-free license to host, copy, format, display, and otherwise use Customer Content only to provide, secure, support, and improve the Restaurant Service and to display Customer's business in ServeGuard's diner discovery experience.
2. Customer represents that it has all rights and permissions needed for Customer Content and that Customer Content is accurate, lawful, not misleading, and not infringing. Ingredient, allergen, dietary, menu, and availability information must be kept current. ServeGuard may remove or restrict content that reasonably appears unlawful, unsafe, deceptive, infringing, or technically harmful.
3. ServeGuard may parse menu files to create editable menu records. The original uploaded menu source file is scheduled for deletion no later than 30 days after upload. Parsed menu records and Customer-approved menu items remain until Customer deletes them or the applicable account is deleted, subject to legal retention requirements.
4. Customer permits display of its business name, logo, location, hours, cuisine, menus, photos, and verification status in the Restaurant Service. ServeGuard will not use Customer's name, logo, testimonials, or identifiable diner data in external advertising or promotional campaigns without separate written or electronically recorded consent. A signed Order Form or marketing release may provide that consent.
5. Suggestions and feedback about the Restaurant Service may be used without restriction or compensation, provided ServeGuard does not publicly identify Customer as the source without permission.

7. Customer personnel data and monitoring

Customer is responsible for giving owners, managers, staff, contractors, and other users any notices and obtaining any consents required for account administration, security logs, table assignments, training records, communications, and workplace use. Customer must not use the Restaurant Service for covert monitoring or unlawful employment decisions. Customer personnel account and assignment information generally remains until Customer deletes it, the employee completes an in-app deletion request, or the organization account is deleted. An employee deletion request removes operational access immediately and schedules permanent account deletion after seven days unless the employee cancels during that recovery window. An authorized manager may separately remove employee access and the linked account immediately. Security and audit logs may be retained for up to 24 months, or longer when reasonably necessary for security, dispute resolution, legal compliance, or enforcement.

8. Fees, renewals, taxes, and payment

1. Customer will pay the fees and taxes stated in the applicable Order Form, checkout flow, invoice, or subscription confirmation. Plans may be monthly, annual, or invoiced under a signed agreement. Unless an Order Form states otherwise, fees are charged in advance and are nonrefundable except where required by law or expressly stated in these Terms.
2. Paid subscriptions automatically renew for successive periods of the same length unless Customer cancels before the renewal date. ServeGuard will disclose any trial conversion and recurring charge before Customer enrolls. Cancellation takes effect at the end of the then-current paid period unless applicable law or an Order Form requires otherwise.
3. ServeGuard may change fees for a future renewal period by giving at least 30 days' notice. Customer authorizes ServeGuard and its payment processor to charge the payment method on file for recurring fees, taxes, and authorized adjustments.
4. Customer is responsible for applicable sales, use, excise, and similar taxes, excluding taxes on ServeGuard's net income. Past-due amounts may accrue lawful collection costs and may result in suspension after reasonable notice. Customer must raise a good-faith billing dispute promptly and pay undisputed amounts.

5 Payment processing is provided by Stripe or another disclosed processor. ServeGuard does not store full payment-card numbers in the Restaurant Service.

9. Subscription cancellation and account deletion

1 Customer must cancel active subscriptions or resolve invoiced commitments before final account deletion. Canceling a subscription does not itself delete the account, and requesting account deletion does not by itself cancel charges already owed.

2 When an authorized owner requests deletion and completes required security verification, the account is scheduled for deletion after a 30-day recovery period. Access may be restricted during that period. Only an authorized owner may request deletion or restoration.

3 If an authorized owner signs in and asks to stop deletion, ServeGuard will place the request in its private administrative console as a priority support action, direct the owner to contact support@serveguardapp.com, and extend the pending-deletion period to 60 days while ownership and authorization are reviewed. Restoration is not guaranteed if the request is incomplete, fraudulent, unlawful, or made after deletion has completed.

4 During a deletion archive, ServeGuard may retain the minimum information needed to secure, restore, bill, or administer the account. Restaurant-facing allergy records continue to expire on their original 90-day schedule and are not extended merely because the account is archived. After final deletion, ServeGuard may retain deidentified data, financial records, security logs, records required by law, and backup copies that are isolated and deleted through ordinary rotation.

10. Security and incidents

ServeGuard uses commercially reasonable administrative, technical, and physical safeguards appropriate to the Restaurant Service, which may include encryption in transit and at rest through its infrastructure providers, role-based access, authentication controls, logging, environment separation, secure development practices, and vendor review. No system is completely secure, uninterrupted, or immune from attack. Customer must maintain reasonable security for its devices, networks, credentials, QR displays, personnel, and exported records.

Each party will promptly notify the other of a confirmed security incident involving the other party's data when notification is required by the DPA or applicable law, cooperate reasonably in investigation and remediation, and avoid misleading public statements. Customer may not conduct penetration testing, vulnerability scanning, or other security testing without ServeGuard's prior written authorization. Good-faith reports should be sent to security@serveguardapp.com if available, or support@serveguardapp.com.

11. Acceptable use

Customer and its users must not:

- violate law or another person's rights;
- submit false, fraudulent, threatening, discriminatory, defamatory, infringing, or malicious content;
- access data, accounts, locations, or systems without authorization;
- probe, scan, reverse engineer, bypass, disable, overload, scrape, or interfere with the Restaurant Service or its security controls, except to the limited extent a restriction is prohibited by law;
- distribute malware, automated traffic, spam, or deceptive QR codes;
- resell, sublicense, or provide the Restaurant Service as a service bureau without written permission;
- use sensitive data for advertising, profiling, data brokerage, or AI-model training; or

- use the Restaurant Service to make medical decisions or represent that ServeGuard provides medical advice or safety certification.

12. Availability, support, changes, and suspension

1. ServeGuard may update, improve, discontinue, or change features. Unless an Order Form expressly provides a service level, no uptime or support-response service level applies. Planned and emergency maintenance, third-party outages, device limitations, connectivity, and events outside reasonable control may affect availability.
2. ServeGuard may suspend access immediately when reasonably necessary to address a security risk, unlawful conduct, payment failure, material misuse, threat to diners or others, or legal requirement. When practicable, ServeGuard will give notice and a reasonable opportunity to cure. ServeGuard may terminate for an uncured material breach, insolvency, repeated misuse, or when continued service would create unreasonable legal or security risk.
3. Customer may stop using the Restaurant Service and cancel according to its plan. Sections that by their nature should survive will survive, including payment obligations, confidentiality, data restrictions, ownership, disclaimers, liability limits, indemnification, dispute resolution, and general provisions.

13. Third-party services and application stores

The Restaurant Service may rely on third-party infrastructure, authentication, payment, communications, mapping, or app-store services. Their terms and privacy practices may apply to Customer's direct relationship with them. ServeGuard is not responsible for a third party's independent service, but remains responsible for its obligations concerning subprocessors under the DPA.

If downloaded from Apple's App Store, these Terms are between Customer and ServeGuard, not Apple. Apple has no obligation to provide maintenance or support and is not responsible for claims relating to the Restaurant Service. To the extent required by Apple's standard terms, Apple and its subsidiaries are third-party beneficiaries of these Terms and may enforce the applicable app-store provisions.

14. Intellectual property

ServeGuard and its licensors own the Restaurant Service, software, designs, workflows, documentation, marks, and related intellectual property, excluding Customer Content. Subject to these Terms and payment of applicable fees, ServeGuard grants Customer a limited, nonexclusive, nontransferable, revocable right during the subscription term to use the Restaurant Service for Customer's internal business operations. No rights are granted by implication. "ServeGuard" and related marks may not be used except as expressly allowed in brand guidance or written permission.

15. Mutual confidentiality

"Confidential Information" means nonpublic information disclosed by one party that should reasonably be understood as confidential, including business plans, security information, pricing, technical information, and personal data. The receiving party will use Confidential Information only to perform or exercise rights under the agreement, protect it using at least reasonable care, and disclose it only to personnel and contractors who need to know and are bound by confidentiality obligations. These duties do not apply to information the receiving party can document was lawfully known without restriction, independently developed, publicly available without breach, or lawfully received from a third party. A legally compelled disclosure is permitted after advance notice when lawful and reasonable assistance at the disclosing party's expense.

16. Warranties and disclaimers

Each party represents that it has authority to enter the agreement. ServeGuard warrants that it will provide the Restaurant Service in a professional and workmanlike manner. Customer's exclusive remedy for breach of that warranty is re-performance or, if ServeGuard cannot reasonably cure, termination and a prorated refund of prepaid fees for the affected unused period.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, EXCEPT FOR THE EXPRESS WARRANTY ABOVE, THE RESTAURANT SERVICE IS PROVIDED "AS IS" AND "AS AVAILABLE." SERVEGUARD DISCLAIMS ALL IMPLIED OR STATUTORY WARRANTIES, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, QUIET ENJOYMENT, AND WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE. SERVEGUARD DOES NOT WARRANT THAT THE RESTAURANT SERVICE WILL BE UNINTERRUPTED, ERROR-FREE, COMPLETELY SECURE, OR SUFFICIENT TO PREVENT AN ALLERGIC REACTION, FOOD-SAFETY EVENT, MISCOMMUNICATION, OR LOSS. CUSTOMER IS RESPONSIBLE FOR ITS FOOD, OPERATIONS, PERSONNEL, AND SAFETY DECISIONS.

Some jurisdictions do not allow certain disclaimers, so they apply only to the extent permitted.

17. Limitation of liability

TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY WILL BE LIABLE UNDER THE AGREEMENT FOR INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR FOR LOST PROFITS, REVENUE, BUSINESS, GOODWILL, OR DATA, EVEN IF ADVISED OF THE POSSIBILITY.

EXCEPT FOR THE EXCLUDED CLAIMS BELOW, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THE AGREEMENT WILL NOT EXCEED THE FEES PAID OR PAYABLE BY CUSTOMER TO SERVEGUARD FOR THE RESTAURANT SERVICE DURING THE 12 MONTHS BEFORE THE EVENT GIVING RISE TO LIABILITY. IF CUSTOMER USED ONLY A FREE SERVICE, SERVEGUARD'S AGGREGATE LIABILITY WILL NOT EXCEED ONE HUNDRED U.S. DOLLARS.

For a party's breach of confidentiality or data-protection obligations under the DPA, the aggregate cap is two times the general cap above. The exclusions of consequential damages and the caps do not apply to Customer's payment obligations; either party's fraud, willful misconduct, or gross negligence; Customer's infringement or misuse of ServeGuard intellectual property; liabilities that cannot lawfully be limited; or a party's indemnification obligations to the extent stated below. These allocations are an essential basis of the agreement.

18. Indemnification

1. Customer will defend, indemnify, and hold harmless ServeGuard and its affiliates, personnel, and contractors from third-party claims, losses, judgments, penalties, and reasonable legal fees arising from Customer's food, ingredients, preparation, cross-contact, premises, service decisions, legal violations, Customer Content, Customer's breach of Sections 3 through 7 or 11, or Customer's users' misuse of the Restaurant Service, except to the extent caused by ServeGuard's breach, gross negligence, or willful misconduct.
2. ServeGuard will defend Customer from a third-party claim that the unmodified Restaurant Service, when used as authorized, directly infringes a United States patent, copyright, or trademark, and will pay finally awarded damages or approved settlements. ServeGuard may modify or replace the affected feature or terminate it with a prorated refund. This obligation does not apply to Customer Content, combinations not supplied by ServeGuard, unauthorized modifications or use, continued use after notice, or compliance with Customer instructions.
3. The indemnified party must promptly notify the indemnifying party, provide reasonable cooperation at the indemnifying party's expense, and allow control of the defense and settlement. No settlement may admit fault by or impose nonmonetary obligations on the indemnified party without its consent, not to be unreasonably withheld.

19. Dispute resolution; arbitration; class waiver

PLEASE READ THIS SECTION CAREFULLY. IT REQUIRES INDIVIDUAL ARBITRATION AND LIMITS HOW DISPUTES MAY BE RESOLVED.

Before filing a claim, the complaining party must send a written notice describing the facts, requested relief, and contact information to legal@serveguardapp.com and allow 30 days for good-faith informal resolution. If unresolved, any dispute arising from the agreement will be resolved by binding arbitration administered by the American Arbitration Association under its Commercial Arbitration Rules by one arbitrator. Arbitration may occur remotely unless the arbitrator determines an in-person hearing is necessary. The place of arbitration is Fulton County, Georgia, subject to the arbitrator's authority and applicable law.

Claims must be brought only on an individual basis. Neither party may bring or participate in a class, collective, consolidated, coordinated, mass, or representative action, and the arbitrator may award relief only to the individual party and only as necessary to resolve that party's claim. The arbitrator, not a court, decides issues of arbitrability, except a court decides the enforceability of the class waiver.

Either party may bring an eligible individual action in small-claims court or seek temporary or preliminary injunctive relief in court to protect confidential information, security, or intellectual-property rights. EACH PARTY WAIVES TRIAL BY JURY TO THE EXTENT PERMITTED BY LAW. If any part of this section is unenforceable, it will be severed to the minimum extent necessary, but no class or representative arbitration may proceed without both parties' written agreement.

20. Governing law and venue

The Federal Arbitration Act governs Section 19. Otherwise, Georgia law governs without regard to conflict-of-law rules. For disputes not required to be arbitrated, the parties consent to exclusive jurisdiction and venue in the state or federal courts located in Fulton County, Georgia, and waive objections to personal jurisdiction or inconvenient forum.

21. Changes to these Terms

ServeGuard may update these Terms for legal, security, operational, or product reasons. Material changes will be provided through the Restaurant Service, email, or another reasonable channel before they take effect. Changes will not retroactively reduce agreed protections for previously collected personal data. If Customer objects to a material change, Customer must stop using the affected Restaurant Service and cancel before the change takes effect. Continued use after the effective date constitutes acceptance where permitted by law. ServeGuard may require renewed click-through acceptance.

22. General terms

Customer may not assign the agreement without ServeGuard's prior written consent, except in connection with a merger or sale of substantially all relevant assets if the successor is not a competitor and assumes all obligations. ServeGuard may assign the agreement to an affiliate or successor. Neither party is liable for delay caused by events beyond reasonable control, except payment obligations. The agreement is the entire agreement about its subject matter and supersedes prior proposals and understandings. Amendments must be in writing or accepted through an authorized electronic workflow. Waivers must be explicit and are not continuing. If a provision is unenforceable, it will be modified to the minimum extent necessary and the remainder remains effective. Headings are for convenience. Electronic records, notices, and signatures satisfy writing requirements where lawful. Customer is responsible for compliance with export-control and sanctions laws.

Formal legal notices must be sent by email to legal@serveguardapp.com and by nationally recognized overnight courier or certified mail to the address below. Routine support and account notices may be sent electronically through the Restaurant Service or to the account email.

23. Contact

ServeGuard LLC 335 Dunhill Way Dr Alpharetta, GA 30005 United States

Support: support@serveguardapp.com Privacy: privacy@serveguardapp.com Legal notices: legal@serveguardapp.com