Table of Contents

12. Third-Party Services & Links

12.1 External Links

12.2 Third-Party Service Providers

13. International Data Transfers

13.1 When International Transfers Occur

13.2 Legal Basis for Transfers

13.3 Safeguards and Oversight

13.4 Your Rights Regarding International Transfers

13.5 Cross-Border Vendor Accountability

13.6 Law-Enforcement and Government Requests

13.7 Data Residency and Backup Regions

13.8 International Cooperation and Compliance

14. Legal Basis for Processing (GDPR & Similar Laws)

14.1 Contract Performance

14.2 Legitimate Interests

14.3 Legal Obligations

14.4 Consent

14.5 Legitimate Interest Assessments

15. Automated Decision-Making

15.1 AI Assessments

15.2 No Harmful Profiling

15.3 Right to Human Review

15.4 Human Review Rights (AI-Related)

16. Privacy Policy Limitations

16.1 Reasonable-Measures Standard

16.2 Events Beyond Our Control (Force Majeure)

16.3 Third-Party Data Handling and Referrals

16.4 Legal and Regulatory Exceptions

16.5 Jurisdiction and Cross-Border Limitations

16.6 Accuracy of Information and Client Responsibilities

16.7 No Waiver of Legal Rights

16.8 Policy Updates and Material Changes

16.9 Contact and Escalation of Concerns

17. Changes to This Privacy Policy

17.1 Right to Modify

17.2 Notice of Changes

17.3 Continued Use

17.4 Version History

18. Contact Information & Data Protection

18.1 Privacy Inquiries

18.2 Data Protection Officer

18.3 Response Timeframe

18.4 Supervisory Authority

alpaca-crew | Privacy Policy

Effective Date: 6/1/2026
Last Updated: 10/25/2025

This Privacy Policy explains how alpaca-crew collects, uses, shares, and protects your information when you use our services. We directly employ trained staff who perform cleaning services and property assessments, supported by our proprietary AI-powered reporting technology.

Understanding Our Business Model: alpaca-crew is a professional cleaning and property assessment service company. We directly employ W-2 staff (service specialists and assessors) who work on variable schedules based on confirmed work availability. This Privacy Policy covers information collected and processed by alpaca-crew in providing our services.

By engaging our services or using our website, you agree to this Privacy Policy.

0.1 Additional Privacy Disclosures

These disclosures supplement the main sections of this Privacy Policy and outline specific rights and obligations required under privacy laws such as the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

They apply to all individuals whose information is collected or processed by alpaca-crew, regardless of where they reside, to the extent those laws apply.

0.2 CCPA/CPRA Disclosures (California Residents)

This section applies to California residents and explains your rights and our obligations under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) for the preceding 12 months and on a going-forward basis.

Notice at Collection

We collect personal information directly from you (e.g., bookings, service communications), automatically (e.g., site analytics), and from service providers or contractors involved in delivering services you request. We collect only what is reasonably necessary for the purposes described below.

Categories of Personal Information We Collect

Depending on your interactions with us (client, site visitor, employee/applicant, or referred partner), we may collect:

- **Identifiers & Contact Details:** name, email, phone, service address, account identifiers.
- **Customer Records / Billing:** payment card tokens, billing address, transaction history (processed by payment processors).
- **Service & Commercial Information:** bookings, service notes, AI report identifiers, add-on selections, referral requests, support communications.
- **Property & Assessment Data:** photos, on-site observations, condition notes, AI-generated recommendations and tiering.
- **Internet / Network Activity:** pages viewed, session identifiers, device/browser metadata, cookie IDs.
- **Geolocation (service logistics):** generalized routing/location relevant to scheduled services.
- **Audio/Visual:** property documentation photos, recorded customer support calls (if applicable and disclosed).
- **Professional / Employment Information:** for employees/contractors (see Section 10.2).
- **Sensitive Personal Information (SPI):** access codes/lockbox combinations, account credentials (hashed), precise geolocation used for routing, and faces incidentally captured in photos (we do not use facial recognition or biometric profiling).

Categories we do not collect: government IDs (SSN/Driver's license/passport), medical/health data, genetic data, union membership, or contents of private communications (beyond support interactions).

Purposes for Which We Use Personal Information

- **Service Delivery:** scheduling, access coordination, cleaning and assessment tasks, post-service documentation.
- **AI-Assisted Reporting:** generating property observations and recommendations (with human review per Section 15.4).
- **Account, Payments & Support:** invoicing, refunds, customer service, recordkeeping.
- **Security & Fraud Prevention:** identity checks, access management, abuse/spam detection.
- **Quality & Improvement:** analytics, troubleshooting, training, safety and policy compliance.
- **Legal & Compliance:** tax/accounting, regulatory responses, claims handling, dispute resolution.

Sources of Personal Information

- **You:** forms, emails, calls, messages, on-site communications.
- **Automatic Collection:** cookies/analytics, device/browser interactions.
- **Service Providers/Processors:** scheduling, payments, hosting, communications.

- **Contractors (at your request):** estimates/fulfillment for referrals you opt into.
- **Employees/Applicants:** HR/operations systems (see Section 10.2).

Disclosures of Personal Information

We disclose personal information for business purposes to:

- **Service Providers / Processors** (e.g., Jobber for scheduling, Stripe/PayPal for payments, cloud hosting, messaging) under written agreements requiring confidentiality, limited use, security, and deletion/return at contract end (see Section 3.2).
- **Contractors (Referrals)** only with your explicit opt-in to share limited property data needed to provide an estimate (see Section 3.3).
- **Analytics Providers** for site performance and measurement (opt-out available).
- **Authorities / Legal** when required by law, court order, or to protect safety/rights.
- **Corporate Events** (merger, acquisition) with notice and subject to this Policy.

We do not provide personal information to data brokers.

"Sale" or "Sharing" Under CPRA

We do not sell personal information in the conventional sense. However, CPRA defines "sale" and "sharing" broadly, which can include disclosures for cross-context behavioral advertising or certain referrals. The only scenarios that may fit "sharing" (or, in limited circumstances, "sale" under CPRA) are:

- **Analytics/Advertising technologies** used to measure site performance or reach (you may opt out).
- **Contractor referrals** you request (limited property data shared to obtain a quote). This may be deemed a "sale" under CPRA even without compensation. You can opt out and/or decline referrals (see Section 3.3 and 0.3).

We do not knowingly sell or share the personal information of minors under 16.

Sensitive Personal Information (SPI) – Limitation

We use SPI only for essential operational purposes (e.g., access codes to complete service, routing for arrival). You may submit a Limit SPI request at any time (see Section 0.3). Where feasible, we minimize SPI by using tokens, restricted fields, and access controls.

De-identified, Aggregated, and Anonymized Data

We may de-identify or aggregate information for analytics, safety, and service improvement (including AI model evaluation). We do not attempt to re-identify de-identified data and maintain safeguards and technical controls to prevent re-identification.

Your CCPA/CPRA Rights

Subject to exceptions, California residents have the right to:

- **Know / Access:** the categories and specific pieces of personal information collected, sources, purposes, and categories of recipients.
- **Correct:** inaccurate personal information.
- **Delete:** personal information (we may retain where legally required or for security/fraud prevention).
- **Opt Out of "Sale"/"Sharing":** including analytics/advertising and contractor referrals (prospective).
- **Limit SPI:** restrict sensitive data use to necessary operational purposes.
- **Non-Discrimination:** you will not be denied goods/services or charged different rates for exercising rights.
- **Authorized Agent:** submit requests through an authorized agent with proof of authorization.

How to Exercise Your Rights

- **Web:** [Privacy Request Form] / [Do Not Sell or Share My Information] / [Limit SPI]
- **Email:** support@alpaca-crew.com
- **Phone:** (510) 731-6110

We acknowledge requests within applicable timelines and respond within 45 days (extendable once by up to 45 additional days when reasonably necessary). Opt-out requests for "sale"/"sharing" are processed within 15 business days.

Verification & Household Requests

We verify your identity using information associated with your account and may request additional details or a signed declaration. For authorized agents, we require proof of authorization and may ask you to verify directly. Household requests may require joint verification. If we deny a request, we will explain the reason and how to remedy or resubmit.

Global Privacy Control (GPC)

We honor GPC signals as valid opt-out preferences for "sale"/"sharing." If your browser sends a GPC signal, we apply it to your session and, when reasonably possible, to your account.

Retention

We retain personal information according to our Data Retention rules (see Section 8.1). Factors include legal obligations, dispute resolution needs, security, and operational requirements. SPI is retained only as long as necessary for access coordination or legal requirements.

Financial Incentives

If we offer discounts or loyalty benefits that constitute a financial incentive (see Section 2.10), we will describe material terms, the categories of personal information implicated, and how to opt in/out without penalty.

Minors

We do not knowingly collect personal information from children under **13**. If we learn we have collected information from a child under 13, we will delete it and notify the parent/guardian where practicable.

Appeals / Complaints

If you believe your request was improperly denied, contact support@alpaca-crew.com with subject "CCPA/CPRA Appeal." You may also contact the California Privacy Protection Agency for guidance.

0.3 Your Privacy Choices

This section explains how you can exercise control over the collection, use, disclosure, and retention of your personal information. These rights apply to California residents under the CCPA/CPRA and may also apply to individuals in other jurisdictions offering comparable protections.

Your Opt-Out and Limitation Rights

You may exercise the following choices at any time:

A. Opt Out of Sale or Sharing of Personal Information
You may instruct us not to sell or share your personal information with third parties, including for:

- Analytics, remarketing, or cross-context behavioral advertising;
- Contractor or vendor referrals initiated through our system;
- Data exchange for promotional or partnership purposes;
- Use of personal data to train AI models beyond operational needs.

Opt-outs are honored without discrimination or impact on service access.

B. Limit Use of Sensitive Personal Information (SPI)

You may restrict our use or disclosure of SPI—including property access codes, alarm credentials, precise geolocation, or photos that may reveal biometric identifiers—to strictly necessary operational purposes such as performing requested services, maintaining security, and legal compliance.

C. Withdraw Consent for AI Training or Profiling Uses

If you previously consented to anonymized or de-identified data being used for algorithmic improvement, you may withdraw that consent prospectively.

D. Restrict Third-Party Analytics and Cookies

You may disable non-essential analytics or advertising cookies through the site's cookie banner or by adjusting browser settings.

How to Submit Opt-Out or Limitation Requests

You may exercise your rights through any of the following:

- **Web Forms:**
    - "Do Not Sell or Share My Personal Information"
    - "Limit the Use of My Sensitive Personal Information"
    - "Opt Out of AI Training Data Use"
- **Email:** support@alpaca-crew.com
- **Phone:** (510) 731-6110

Requests may also be submitted by an authorized agent with proof of authority. If we cannot verify your identity, we will provide an explanation and instructions to complete verification.

Processing Timeline and Verification

- Acknowledgment within 10 business days.
- Completion within 15 business days from receipt of verification.
- Opt-outs take effect prospectively and are binding for at least 12 months unless you re-authorize sharing.
- We may request identity verification or signed declaration for sensitive requests.
- If additional time is needed, we will notify you and provide an estimated completion date (within a maximum of 45 days).

Global Privacy Control (GPC)

We recognize and honor Global Privacy Control (GPC) signals. When your browser or extension transmits a valid GPC signal, we automatically treat it as an opt-out of "sale" and "sharing." Your preference is applied to the specific browser/device session and, if possible, to your account records.

You may update GPC settings at https://globalprivacycontrol.org.

Effect of Opt-Outs and Limitations

Exercising these choices will not:

- Affect your ability to schedule or receive services.
- Change your pricing or discount eligibility.
- Limit our ability to perform core operations such as billing, fraud prevention, and legal compliance.

Certain features that rely on data sharing (e.g., AI recommendations, predictive maintenance alerts, referral matching) may be disabled as a result of your choice.

Verification for Authorized Agents

Authorized agents must provide:

- Signed authorization from the consumer, and either (a) proof of power of attorney or (b) verified identity of the consumer.
- We may require the consumer to directly confirm authorization for security purposes.

Data Retention for Opt-Out Records

We retain records of opt-out and limitation requests for at least 24 months to demonstrate compliance, including date and method of submission and outcome.

These records are stored separately from active service files and are used only for audit and regulatory purposes.

Appeals and Complaints

If you believe your opt-out or limitation request was not honored, you may appeal by emailing support@alpaca-crew.com with subject "CCPA Appeal."

We will review within 30 days and notify you in writing of the outcome and further recourse options.

You may also contact the California Privacy Protection Agency (CPPA) for assistance.

---

1. Information We Collect

We collect information necessary to provide services, generate AI-powered property insights, process payments through our platform (Jobber), and manage contractor referrals.

1.1 Personal Information

Name, phone number, email address, and property address to confirm bookings, coordinate with our staff, send service updates, and deliver reports.

1.2 Service Information

Service preferences, special instructions, visit frequency, and customized care plan details to provide services and tailor recommendations.

1.3 Payment Information

Billing details, invoices, transaction records, and payment history processed through our platform (Jobber) to manage payments, including:

- Service charges for cleaning and assessment services
- Optional gratuities that clients choose to add for employees

Gratuity Processing: When clients add gratuities through our payment system, we collect and process these amounts solely for the purpose of distributing them to employees. We track these transactions separately to ensure 100% distribution to employees and proper tax reporting. We retain no portion of gratuities processed through our system.

Direct Gratuities: We do not collect, process, or track gratuities that clients provide directly to employees outside our payment system. Such transactions occur independently and are not recorded in our systems.

1.4 Property Data Collected by Our Staff

During cleaning, maintenance, or assessment visits, our assessors and service specialists may collect photos, written observations, and condition data to document visible property status, record service completion, and support AI-assisted reports.

Purpose and Scope of Collection

We collect property-related data solely to:

- Provide and document cleaning and assessment services;
- Generate AI-powered property reports, maintenance insights, and tier classifications;
- Track condition trends across recurring visits;
- Support quality-assurance reviews and training;
- Investigate service concerns or insurance claims; and
- Meet regulatory or contractual obligations.

We do not use property images or observations for unrelated marketing, employee surveillance, or behavioral analytics.

Types of Property Data Collected

Depending on service scope, data may include:

- Digital photographs or short video clips of relevant interior or exterior areas;
- Written notes on visible wear, damage, or maintenance needs;
- AI-generated annotations identifying potential risks or required follow-up;
- Surface or cleanliness ratings used for internal benchmarking; and
- Metadata (timestamp, device ID, GPS routing for job verification).

We do not intentionally photograph private areas (bedrooms, bathrooms, medicine cabinets) unless required for cleaning documentation.

Biometric and Visual Data Notice

Property photos may incidentally capture identifiable features, such as faces, tattoos, license plates, or household items.

Under laws such as California Civil Code §1798.140, Illinois BIPA, and Texas §503.001, these may qualify as biometric identifiers.

To ensure compliance and minimize risk:

- We do not use facial-recognition or biometric-profiling software.
- We do not tag, match, or index images to personal identities.
- Any automated face-detection tools are used only to flag and blur human faces before storage.
- All visual files are encrypted at rest (AES-256) and in transit (TLS/SSL).
- Access is limited to authorized quality-assurance or AI-processing staff under confidentiality agreements.

Notice Before Collection (Required by Law)

Before collecting any photo or observation data, clients are informed that:

1. Photos may incidentally include individuals present on-site.
2. The purpose is property documentation, not personal surveillance.
3. Data is retained for service, audit, and legal compliance purposes.
4. Clients may opt out or request face-redaction before service.

Retention and Deletion Schedule

Property photos and related condition data are retained for:

- Active clients – for the duration of the service relationship + 7 years;
- Inactive clients – 7 years after the last service;

- Extended retention if required for legal claims, audits, or regulatory holds.

Upon verified deletion request or expiration of the retention period:

- All copies are securely deleted or anonymized;
- Backups are overwritten within 90 days;
- Audit logs are maintained confirming destruction.

Opt-Out or Restriction Options

You may request to:

- Exclude all photo documentation before service begins;
- Redact identifiable images (faces, license plates, artwork);
- Restrict AI-based analysis of collected images; or
- Delete previously captured property media (subject to legal holds).

Submit requests to support@alpaca-crew.com before scheduling or anytime thereafter.
If you opt out, we can still provide cleaning and manual reports, but AI-generated analytics and condition-tracking features will be disabled.

Consent and Legal Basis

By engaging our services after receiving this notice, you provide **informed consent** for limited photo and observation data collection as described. Consent may be withdrawn prospectively at any time.

Security and Access Controls

- Encrypted storage on cloud servers with role-based access control.
- Multi-factor authentication for all user accounts accessing property data.
- Quarterly audits of access logs and retention compliance.
- Incident-response plan in accordance with Section 5.4 (Data Breach Response).

Disclosure to Third Parties

Property photos and condition data may be disclosed only:

- To service providers (e.g., Jobber, cloud hosting, AI-processing vendors) under data-processing agreements;
- To referred contractors – only with your explicit request (see Section 3.3);
- To insurers or legal counsel for verified damage or liability claims; or
- As required by law, subpoena, or safety-related exigency.

We do not sell, trade, or monetize property or image data.

Children's and Household Privacy

We do not knowingly retain identifiable images of minors.

If a photo inadvertently captures a child under 13, we will:

- Notify the parent/guardian,
- Delete or blur the image immediately, and
- Honor any future opt-out request.

Household members who are not direct clients may contact us to request redaction or deletion of images in which they appear.

Contact for Biometric or Visual-Data Inquiries

Email: support@alpaca-crew.com
Subject Line: "Biometric or Property Photo Inquiry"

We respond within 10 business days with confirmation or next steps.

1.5 Assessment-Specific Data

During paid on-site assessments conducted by our assessors, the following data is systematically collected:

- Detailed photographs of property conditions
- Standardized evaluation criteria and condition ratings
- Notes on visible wear, damage, maintenance needs, and potential risks
- Measurements and spatial documentation when relevant

This assessment data is processed by alpaca-crew's proprietary AI system for report generation and personalized care planning.

1.6 Client-Submitted Information

Information, photos, descriptions, and property details submitted by clients through Request Forms on our website. This data may be used for quote generation and, for assessment clients, incorporated into AI analysis.

1.7 Website Usage Data

Pages visited, links clicked, time spent on site, and interaction patterns to improve website functionality and user experience.

1.8 Communication Records

Customer support interactions including inquiries, complaints, feedback, service requests, and resolution outcomes.

1.9 Location Data

Service location information and, when applicable, routing data from our staff arriving at and departing from properties, used for scheduling verification and service coordination.

1.10 Voice Records

Phone calls with alpaca-crew may be recorded for quality assurance, training, and dispute resolution purposes. You will be notified when calls are recorded.

1.11 Incidental Information

During service delivery, our staff may inadvertently observe personal information present in client properties. alpaca-crew does not intentionally collect such information, and any incidental observations are not systematically recorded or used beyond immediate service delivery needs.

1.12 Employee Information

Information about our employees, including contact information, service performance records, quality audit results, training records, and payment details for employment and business operations.

---

2. How We Use Your Information

2.1 Service Delivery

Process bookings, schedule our staff through our platform (Jobber), manage service delivery, conduct quality oversight, generate AI-powered reports from data collected by our assessors, and facilitate contractor referrals when requested.

2.2 AI Analysis & Reporting

For clients who complete paid assessments, we use property data collected by our assessors to:

- Generate AI-powered property condition reports using our proprietary technology
- Track condition changes over time through longitudinal analysis
- Provide personalized maintenance recommendations
- Identify patterns and trends in property care needs
- Create tier classifications reflecting property condition

2.3 Business Operations

Manage our business including scheduling through Jobber, payment processing, rewards program administration, quality standards enforcement, and employee coordination.

2.4 Service Improvement

Review aggregated client data to understand service preferences, monitor property care trends, improve AI algorithms, enhance platform functionality, and improve overall service quality.

2.5 Communication

Send appointment reminders, service updates, assessment results, AI reports, and with your consent, promotional content about new services or offers.

2.6 Employee Management

Share necessary information with our employees to enable service delivery, quality oversight, training, and performance evaluation.

2.7 Security & Fraud Prevention

Monitor for unauthorized access, detect fraudulent activity, prevent account misuse, and protect client and business information.

2.8 Legal Compliance

Meet contractual obligations, comply with regulatory requirements, respond to legal processes, and maintain required business records.

2.9 Quality Assurance

Monitor service quality through assessor audits, verify service completion, ensure compliance with standards, and coordinate issue resolution.

2.10 Rewards Program Disclosure

We offer a voluntary rewards program designed to recognize recurring clients through periodic discounts, loyalty credits, or service incentives. This section explains how we collect and use your information in connection with these benefits and outlines your rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)**.**

Nature of the Program

The rewards program may include:

- Service discounts or loyalty credits for recurring bookings.
- Exclusive offers for long-term or referral-based clients.
- Anniversary or milestone-based promotions.
- Referral or feedback-based incentives.

Participation is entirely optional**,** and declining participation will not affect your access to regular services, pricing, or eligibility for standard promotions available to all customers.

Categories of Personal Information Collected

To administer and maintain rewards participation, we may collect:

- Identifiers and contact details (name, email, phone number).
- Account and booking history (service dates, frequency, property type).
- Payment and invoice records to confirm eligibility.
- Participation metrics (points earned, redeemed, or expired).
- Communication preferences (email or text notification opt-ins).

We do not collect additional sensitive personal information solely for the rewards program beyond what is required for service administration.

Purpose of Collection and Use

Your data is used solely to:

- Track your rewards balance and redemption eligibility.
- Apply credits or discounts to invoices.
- Communicate account updates, tier changes, or special offers.
- Verify participation activity and resolve any discrepancies.
- Fulfill legal obligations regarding financial reporting and record retention.

We do not use rewards-program data for advertising unrelated to our services.

Disclosure and Retention

Rewards-program data may be disclosed to:

- **Payment processors** (to apply discounts or credits to invoices).
- **CRM and scheduling platforms** (to track participation and service frequency).
- **Customer support staff** (for account management).

All such third parties act as service providers under written agreements restricting use, retention, and further disclosure of data.

Rewards data is retained for as long as your account remains active and for up to seven (7) years thereafter for recordkeeping, tax, and compliance purposes.

Financial Incentive Notice

Under CCPA §1798.125**,** this program may be considered a "financial incentive" because participants receive monetary or service-related value in exchange for the collection and use of limited personal information (e.g., contact and service history).

We estimate the value of your data based on:

- The cost of administering the program and average incentive value offered.
- The average revenue generated from program participation.
- The operational benefit derived from loyalty retention.

The incentives offered are reasonably related to the value of the personal data provided and are not unfair, deceptive, or coercive.

Non-Discrimination Assurance

We will never:

- Deny you services or quality based on your participation or opt-out status.
- Charge different prices or impose penalties for exercising privacy rights.
- Provide a lower level of service to non-participants.

Participation is voluntary and may be terminated at any time without consequence to your regular service relationship.

Opt-In and Opt-Out Rights

You may opt in by completing a rewards enrollment form, responding to a promotional invitation, or confirming participation through your client account.

To opt out, you may:

- Email support@alpaca-crew.com with subject line "Opt Out of Rewards Program."
- Call (510) 731-6110 to request manual removal.
- Decline or ignore enrollment invitations.

Upon opt-out, your rewards data will be deleted or anonymized within 45 days**,** except for legally required accounting records.

Withdrawal of Consent

You may withdraw your consent for data processing under the rewards program at any time. Withdrawal does not retroactively affect previously applied rewards but will terminate future accumulation of benefits.

Your Rights Under CCPA/CPRA

You have the right to:

- Request access to the categories and specific pieces of information collected about you for the rewards program.
- Request correction or deletion of such information.
- Obtain an explanation of the material terms, categories of data used, and estimated value of the incentive.
- File a complaint with the California Privacy Protection Agency (CPPA) if you believe your rights were violated.

We verify all such requests before processing and respond within 45 days, extendable by law.

Contact Information

Questions about this rewards program or your rights under CCPA/CPRA can be directed to:

Email: support@alpaca-crew.com
Phone: (510) 731-6110
Mailing Address: 548 Market Street, PMB 948619, San Francisco, CA 94104

---

3. Sharing Your Information

We do not sell or rent your personal information. We share information only as necessary for service delivery, employee management, legal compliance, or security purposes.

3.1 Our Employees

We share necessary property and client information with our employees (assessors and service specialists) who perform services at your property. Our staff receive:

- Property access information
- Service scope and special instructions
- Relevant property condition information
- Quality standards and expectations

All employees are bound by confidentiality obligations and trained to handle information according to this Privacy Policy.

3.2 Platform Service Providers

We engage carefully selected service providers and subcontracted processors to help operate, secure, and enhance our services. These providers perform functions such as scheduling, payment processing, cloud hosting, analytics, communication delivery, and AI-supported reporting.

We remain responsible for the actions and safeguards of all providers that process information on our behalf and require each to handle data in accordance with this Privacy Policy and applicable privacy laws.

Categories of Service Providers

Depending on your interaction with our platform, your data may be processed by:

- **Scheduling and CRM Platforms** – Jobber, HubSpot, or similar tools for scheduling, invoicing, and form submissions.
- **Payment Processors** – Stripe, PayPal, or similar processors for secure transaction handling, refunds, and charge dispute resolution.
- **Cloud and Infrastructure Hosts** – Amazon Web Services (AWS), Google Cloud, and similar platforms for encrypted data storage and system availability.
- **Communication Providers** – Twilio or comparable vendors for email and SMS delivery, including appointment reminders and service notifications.
- **Analytics & Website Optimization Tools** – limited, aggregated usage data to assess site performance and troubleshoot issues.
- **Cybersecurity Partners** – vendors providing network monitoring, intrusion detection, and encryption key management.

We maintain a record of all active service providers and their processing purposes. You may request a current list at support@alpaca-crew.com.

Vendor Selection and Due Diligence

Before engaging any third-party processor, we conduct due diligence that includes:

- Review of privacy policies, certifications, and audit reports (SOC 2 / ISO 27001).
- Verification of security architecture, access controls, and encryption methods.
- Assessment of data residency and cross-border transfer mechanisms.
- Confirmation of compliance with CCPA/CPRA, GDPR, and applicable U.S. laws.

Vendors must demonstrate a proven track record of secure operations and data-handling integrity prior to onboarding.

Contractual Safeguards

All vendors operate under legally binding written agreements requiring:

- Processing personal information only for documented, specific purposes consistent with alpaca-crew's instructions.
- Maintaining industry-standard security measures, encryption, and physical protections.
- Prohibiting any sale, secondary use, or independent "sharing" of data.
- Providing prompt notice (no later than 72 hours) of any suspected or confirmed data breach.
- Ensuring that any sub-processors they use provide equivalent contractual protections**.**
- Allowing alpaca-crew or its auditors to verify compliance upon reasonable notice.
- Returning or permanently deleting data when services terminate.

These contractual obligations are designed to satisfy CCPA/CPRA §1798.140(j) and GDPR Article 28 processor requirements.

Data Residency and Cross-Border Transfers

Most platform providers process data within the United States. When international transfers occur (e.g., EU or UK hosting redundancy), we ensure adequate protection by:

- Executing Standard Contractual Clauses (SCCs) or equivalent frameworks approved by the European Commission or UK ICO**;**
- Requiring vendors to adhere to data-minimization and retention limits**;**
- Conducting transfer impact assessments (TIAs) to confirm risk level and compliance; and
- Maintaining internal records of all international transfer decisions.

Clients will be notified if a significant change in cross-border transfer safeguards occurs.

Security and Monitoring

Our providers are required to:

- Encrypt all data at rest (AES-256) and in transit (TLS/SSL).
- Employ multi-factor authentication for administrative access.
- Maintain detailed audit logs and anomaly detection.
- Test and update security protocols regularly.
- Comply with alpaca-crew's Data Breach Response Policy (see Section 5.4).

We conduct periodic security assessments and require certifications or compliance statements annually.

Retention and Data Access

Service providers may only retain data for as long as necessary to perform contracted services or comply with legal obligations.

Access is strictly role-based, logged, and subject to least-privilege principles. Providers must destroy or return personal data upon request or contract termination, with written confirmation of deletion.

Breach Notification and Liability
If a provider experiences a security incident or data breach affecting your personal information, they must:

- Immediately contain the incident and secure data;
- Notify alpaca-crew within 72 hours of discovery;
- Provide details of affected systems, data categories, and mitigation steps; and
- Cooperate fully in investigation, remediation, and regulatory notifications.

Failure to comply with these standards may result in termination of the relationship and potential liability under applicable law.

Your Rights and Our Accountability

You may request information about:

- Which service providers currently process your data;
- The purpose and scope of their processing;
- Applicable safeguards in place for each vendor.

Requests should be submitted to support@alpaca-crew.com with subject line “Platform Service Provider Inquiry.” We will provide a verified response within 45 days.

3.3 Contractor Referrals

When you request repair, maintenance, or specialized service referrals outside the scope of our regular cleaning offerings, we may disclose limited, relevant property information to independent contractors to help you obtain accurate quotes or schedule services.

We value transparency and client choice: no referral occurs without your explicit opt-in consent, and you may opt out at any time.

Purpose of Disclosure

Information is disclosed only to:

- Provide accurate estimates or inspections requested by you;

- Facilitate introductions between you and qualified contractors;
- Support continuity of care for property-maintenance needs; and
- Track referral performance for quality, safety, and compliance purposes.

We do not disclose personal information for unrelated marketing, resale, or data brokerage purposes.

Categories of Information Shared

Depending on the referral requested, we may share:

- Your name, email, and phone number;
- Service address and property access instructions (if you choose to provide them);
- Relevant property photos or videos showing the area to be assessed;
- AI-generated observations or recommendations relevant to the service requested;
- Service tier classification or history (if relevant to pricing or scope).

No payment or financial details are ever shared with contractors.

Categories of Contractor Referrals

1. **Vetted Contractors** – Pre-screened for valid licensing, active insurance, and general alignment with safety and quality standards.
2. **AI-Generated Referrals** – Identified through algorithmic matching based on geography, service type, and availability. These are provided "as is" for convenience and may not be independently verified.

Notice of Potential "Sale" or "Sharing" Under CPRA

Under California law, disclosure of personal information to independent contractors who are not bound as our "service providers" may be considered a "sale" or "sharing" even when no payment is exchanged.

We treat such disclosures as opt-in only and provide a corresponding opt-out right.

You may withdraw consent at any time by emailing support@alpaca-crew.com or using our "Do Not Sell or Share My Personal Information" link.

Consent and Opt-Out Process

Before any referral occurs, we will:

1. Notify you of the intended disclosure and categories of information shared;
2. Identify each contractor or business category involved;
3. Obtain your explicit consent (via email or recorded confirmation); and
4. Provide a clear method to revoke consent later.

Opt-outs are effective within 15 business days and apply prospectively to future referrals.

Contractor Responsibilities and Data Handling

Although contractors operate independently, we contractually require any referred contractor to:

- Use shared information only for providing a quote or performing the requested service;
- Maintain appropriate security controls and confidentiality;
- Not sell or redistribute your data;
- Delete your information within 90 days if no service is performed; and
- Comply with applicable privacy laws (CCPA, CPRA, GDPR if relevant).

However, because these contractors are independent businesses, we cannot guarantee their compliance once data has been shared at your direction.

Limitations of Liability

alpaca-crew does not control, supervise, or employ referred contractors and is not liable for:

- Work quality, pricing, or timelines;
- Contractor data-handling or privacy practices;
- Property damage or injury caused by contractors; or
- Third-party communications between you and contractors.

You are responsible for vetting and contracting directly with the contractor of your choice.

To the maximum extent permitted by law, alpaca-crew is not responsible for any damages arising from contractor services unless caused solely by our own gross negligence or willful misconduct.

Your Responsibilities When Engaging Contractors

Before hiring, you should:

- Verify licensing and insurance status directly with the contractor;
- Review references and public records for complaints or violations;
- Request a written estimate and define scope in a signed agreement;
- Confirm data handling and privacy practices with the contractor; and
- Retain all receipts and communications for future reference.

We encourage you to use only licensed and insured professionals for any project.

Indemnification

By requesting and accepting a referral, you agree to indemnify and hold alpaca-crew harmless from any claims, liabilities, damages, or expenses arising from:

- Work performed by a referred contractor;
- Negligence or misconduct of the contractor; or
- Any dispute between you and the contractor.

This indemnification does not apply to losses arising solely from alpaca-crew's own gross negligence or intentional misconduct.

Record of Disclosures

We maintain records of each contractor referral for a minimum of 24 months, including:

- Date of referral and categories of data shared;
- Identity or business category of contractor; and
- Proof of client authorization.

You may request a copy of your referral record by emailing support@alpaca-crew.com. Verified responses are provided within 45 days.

Regulatory Disclosure – California Residents

Pursuant to Cal. Civ. Code § 1798.140(ad) and § 1798.120:

- You have the right to opt out of any referral considered a "sale" or "sharing."
- We will not discriminate against you for exercising this right.
- We do not knowingly share information about individuals under 16 years of age.

Contact for Contractor Referral Inquiries

Email: support@alpaca-crew.com
Phone: (510) 731-6110
Subject Line: "Contractor Referral Disclosure Inquiry"

3.4 Legal & Regulatory Disclosures

We may disclose information when:

- Required by law, regulation, court order, or valid legal process
- Necessary to respond to government requests or investigations
- Required to comply with tax, business, or regulatory obligations
- Necessary to enforce our Terms of Service or protect our legal rights

3.5 Business Transfers

In the event of a merger, acquisition, sale of assets, or business reorganization, client data may be transferred as part of the transaction. We will notify affected clients and ensure the acquiring party commits to protect information consistent with this Privacy Policy.

3.6 Emergency Situations

We may share information with emergency services, law enforcement, property managers, or other relevant authorities when we believe in good faith that disclosure is necessary to:

- Protect health, safety, or prevent imminent harm
- Prevent illegal activities or respond to security threats
- Address urgent property emergencies requiring immediate action

Such emergency disclosures are limited to information necessary to address the immediate situation.

3.7 Anonymized Data

We may share aggregated, anonymized data that cannot identify individual clients for:

- Business analytics and service improvement
- Industry research and benchmarking
- Marketing and promotional purposes
- AI system training and development

3.8 Third-Party Data Handling Limitations

Important: Once information is shared with referred contractors, alpaca-crew cannot control how those independent parties handle, store, or protect your information. While we contractually require data protection standards from referred contractors, we are not responsible for:

- Contractor data security practices
- How contractors store or transmit data
- Data breaches occurring in contractor systems
- Contractor compliance with privacy laws

---

4. AI-Powered Assessments & Data Processing

Our services include AI-powered property assessment technology designed to provide maintenance insights and track property conditions over time. This section explains how our AI system works, what protections are in place, and what limitations apply.

4.1 Eligibility & Access

AI-powered reports are available exclusively to clients who complete paid on-site assessments conducted by our assessors. Clients who choose Quote Review without assessment do not receive AI reports or ongoing tracking.

4.2 How AI Analysis Works

Our proprietary AI system processes data collected by our assessors to:

- Analyze observable property conditions including cleanliness levels, wear patterns, and maintenance needs
- Compare conditions across multiple visits to identify trends and changes over time
- Generate tier classifications that reflect overall property condition
- Provide personalized maintenance recommendations based on property-specific patterns
- Estimate appropriate service scope and frequency
- Identify potential issues before they become major problems

Data Sources for AI Analysis:

- Photos and observations recorded by our assessors during on-site assessments
- Information and photos submitted by clients through Request Forms
- Observations noted by our service specialists during routine service visits
- Historical service data and condition tracking over time

4.3 What AI Does NOT Do

Our AI systems are designed with specific limitations to protect privacy and set appropriate expectations:

- **No deep structural analysis** - AI does not provide engineering or architectural evaluations
- **No surveillance access** - AI does not access or process security camera footage
- **No personal data processing** - AI does not analyze personal documents, financial records, or identity information
- **No hidden condition detection** - AI cannot see behind walls, under flooring, or in closed systems
- **Not a replacement for professionals** - AI does not provide licensed inspections, certifications, or professional opinions

4.4 Human Oversight & Review

Every AI-generated report undergoes human review by alpaca-crew staff before delivery to clients. This review ensures:

- Report accuracy and clarity

- Appropriate recommendations
- Proper context and explanations
- Removal of any inappropriate content or observations

4.5 Report Security & Access

AI-generated reports are:

- Encrypted during transmission and storage
- Accessible only to the client and authorized alpaca-crew staff
- Stored on secure servers with access controls
- Protected by authentication requirements
- Available for download through secure client portals

Reports may be disclosed to third parties only when:

- The client explicitly requests contractor referrals and consents to sharing
- Required by law or valid legal process
- Necessary for emergency situations

4.6 Client Control & Consent

Clients maintain control over AI analysis:

- **Opt-out rights** - Clients may opt out of AI report generation at any time
- **Report approval required** - AI recommendations do not automatically change service plans without client approval
- **Data access** - Clients can request copies of data used in AI analysis
- **Deletion rights** - Clients can request deletion of AI reports subject to legal retention requirements

4.7 AI Limitations & Disclaimers

Important Limitations:

- AI analysis depends on data quality - incomplete observations, poor lighting, or access restrictions directly affect accuracy
- AI may miss unique or unusual conditions that fall outside training patterns
- AI cannot predict future conditions with certainty
- AI reports may contain errors, omissions, or misinterpretations
- Property conditions may change between assessment dates

Client Responsibility: Clients should never rely solely on AI reports for significant property decisions. AI reports are informational tools that should be verified through:

- Independent professional inspections when making major decisions

- Licensed specialists for structural, environmental, or system evaluations
- Additional assessments when property conditions change significantly

alpaca-crew is not responsible for decisions made based on AI reports without independent professional verification.

4.8 Longitudinal Analysis & Trend Tracking

For clients with multiple service visits, our AI system may:

- Compare property conditions across visits to identify deterioration or improvement
- Track effectiveness of maintenance interventions
- Predict potential future maintenance needs based on observed patterns
- Adjust recommendations based on how property responds to services

This longitudinal analysis helps clients understand property care trends and plan proactive maintenance.

4.9 AI System Updates & Evolution

Our AI systems are continuously refined to improve accuracy and capabilities:

- Updates may change how data is processed or how reports are generated
- System changes may affect comparison accuracy between old and new reports
- We do not guarantee backward compatibility with previous AI versions
- Significant system changes will be reflected in Privacy Policy updates

AI Training Data Retention: Anonymized property condition data used for AI system training and improvement may be retained for up to 10 years to enable long-term algorithm refinement and accuracy enhancement. Individual client data within training sets is de-identified using industry-standard techniques and cannot be reverse-engineered to identify specific properties or clients. We implement technical safeguards including data aggregation, statistical noise injection, and removal of identifying metadata to ensure training data cannot be traced back to individual clients. Clients may request exclusion of their data from future AI training sets by contacting our privacy team.

4.10 Data Processing Minimization

We process only the minimum data necessary for AI analysis:

- Property condition information and maintenance patterns only
- No processing of personal conversations, private documents, or sensitive personal information beyond property care needs
- No use of AI for client profiling beyond property assessment purposes
- No AI analysis of client behavior, preferences, or characteristics unrelated to property services

4.11 Algorithmic Transparency & Bias Mitigation

While our specific AI algorithms are proprietary, we commit to:

- Providing general information about data types processed and analysis performed upon request
- Regularly reviewing AI systems for potential biases
- Implementing corrective measures to ensure fair assessments across different property types
- Testing AI performance across diverse property characteristics and client demographics

---

5. Data Security

We implement multiple layers of security to protect your information, though no system can guarantee absolute protection against all threats.

5.1 Technical Security Measures

Encryption: All data transmitted to and from our systems uses industry-standard encryption protocols (TLS/SSL). Stored data containing sensitive information is encrypted at rest.

Access Controls: Role-based access ensures staff can only access information necessary for their specific functions. Multi-factor authentication required for administrative access to our platform.

Secure Infrastructure: Our systems are hosted on secure servers with firewalls, intrusion detection, and regular security monitoring.

Regular Updates: Security software, systems, and protocols are regularly updated to address emerging threats.

Security Program: We maintain a comprehensive information security program that includes regular security assessments, employee training on data handling, incident response procedures, and third-party security audits of critical systems. While we cannot guarantee absolute security, we commit to commercially reasonable efforts that meet or exceed industry standards for businesses of our size and type. Our security program is reviewed annually and updated to address evolving threats and regulatory requirements.

5.2 Physical Security

Our facilities and equipment are secured against unauthorized physical access through:

- Controlled access to physical locations
- Secure storage of physical records

- Equipment security protocols
- Disposal procedures for sensitive materials

5.3 Security Limitations

No Absolute Guarantee: Despite our security measures, no method of electronic storage or transmission is completely secure. We cannot guarantee absolute protection against:

- Sophisticated cyber attacks
- Zero-day vulnerabilities
- Insider threats beyond our control
- Third-party system compromises

Third-Party Platform Security: Our use of Jobber and other third-party platforms means your information is also subject to their security practices. We select reputable providers but cannot guarantee their security.

5.4 Data Breach Response

We maintain a formal Incident Response and Breach Notification Plan to ensure that any unauthorized access, disclosure, or loss of personal data is detected, contained, investigated, and remedied promptly and transparently.

Definition of a Data Breach

A “data breach” includes any confirmed or suspected event resulting in:

- Unauthorized access to, or acquisition of, personal information;
- Accidental or unlawful destruction, alteration, or disclosure of personal or property-related data;
- Loss or theft of devices or media containing personal data;
- Unauthorized access by contractors, employees, or third-party providers; or
- Compromise of login credentials, API keys, or encryption keys.

Security incidents that do not expose personal data are logged, investigated, and treated as near-miss events to improve prevention measures.

Immediate Response Steps

Upon discovery of a potential breach, alpaca-crew will:

1. **Contain** the incident by isolating affected systems and disabling compromised accounts.
2. **Activate the Incident Response Team (IRT)**, including IT Security, Compliance, Legal Counsel, and Executive Management.
3. **Preserve evidence** (e.g., forensic images, access logs, timestamps).
4. **Engage forensic specialists** and cloud-vendor security teams as necessary.

5. **Assess impact** to determine what personal information, systems, or individuals were affected.
6. **Mitigate harm** through credential resets, firewall rule updates, or other corrective actions.

Internal Investigation and Assessment

Within 72 hours of confirmation, we:

- Identify the breach vector and root cause;
- Determine the number and categories of affected individuals;
- Evaluate potential harm (financial, reputational, or privacy-related);
- Document containment and mitigation measures;
- Coordinate with law enforcement and forensic analysts if criminal activity is suspected.

All findings are retained in an internal Breach Register maintained by the Compliance Officer for a minimum of seven (7) years.

Notification to Affected Individuals

If personal data has been, or is reasonably believed to have been, compromised, we will:

- Notify affected individuals without unreasonable delay, and in any event within timeframes required by law (generally ≤ 45 days in California; ≤ 72 hours for GDPR reportable breaches).
- Deliver notice by email, written correspondence, or public posting if contact information is unavailable.
- Include in each notice:
    - A general description of what occurred;
    - The categories of data involved (e.g., names, addresses, photos, payment tokens);
    - The approximate date range of exposure;
    - Steps we have taken to mitigate the risk;
    - Actions individuals can take to protect themselves (password resets, fraud alerts, etc.); and
    - Contact information for further assistance.

We do not notify affected persons when law enforcement determines that doing so would impede an ongoing investigation; notification will occur promptly once that restriction is lifted.

Regulatory and Third-Party Notifications

We notify, as applicable:

- The California Attorney General and any other state agencies with jurisdiction if the incident affects > 500 residents;

- The California Privacy Protection Agency (CPPA) under CPRA §1798.185;
- The Federal Trade Commission (FTC) for material security failures under the Safeguards Rule;
- European supervisory authorities (within 72 hours) for affected EU/UK data subjects; and
- Our vendors, insurers, and legal counsel for compliance coordination.

Notifications include event details, mitigation steps, and planned preventive actions.

Preventive and Remedial Measures

Following containment, we:

- Conduct root-cause analysis and implement permanent controls;
- Update incident-response and security policies;
- Retrain staff on data protection and phishing awareness;
- Patch vulnerable systems and enhance network segmentation;
- Perform follow-up audits and penetration testing to validate remediation.

Individual Support and Remediation

Where appropriate, we may:

- Offer credit-monitoring or identity-protection services for 12–24 months;
- Assist clients in resetting credentials and strengthening account security;
- Provide dedicated incident-response contacts and updates until resolution.

Breach Communication and Transparency

All breach-related communications will be delivered in clear, concise, non-technical language. We maintain a dedicated email address and hotline for breach inquiries.

Email: security@alpaca-crew.com
Phone: (510) 731-6110
Subject Line: "Data Breach Notification or Security Incident Inquiry"

Retention and Recordkeeping

All documentation—including forensic reports, investigation notes, notifications, and regulatory correspondence—is retained for no less than seven (7) years to demonstrate compliance and continuous improvement.

5.5 Client Security Responsibilities

Clients share responsibility for protecting their information:

- **Property Security:** Secure sensitive documents, valuables, and confidential information before service visits
- **Access Information:** Protect access codes, keys, and entry credentials
- **Account Security:** Maintain confidentiality of login credentials for client portals
- **Device Security:** Ensure devices used to access our services have appropriate security measures

alpaca-crew is not responsible for:

- Information left unsecured on client properties during service visits
- Unauthorized access resulting from shared or compromised access credentials
- Security incidents caused by client device vulnerabilities
- Property security breaches resulting from information shared with our staff

---

6. Your Privacy Rights

You have significant control over how your information is collected, used, and stored.

6.1 Right to Access

Request copies of personal information we maintain about you, including:

- Account and contact information
- Service history and records
- Assessment reports and AI-generated content
- Communication records
- Payment history

6.2 Right to Correction

Request correction of inaccurate, incomplete, or outdated information. We will update records upon verification of corrections.

6.3 Right to Deletion

Request deletion of your personal information, subject to exceptions:

- **We will delete:** Most personal data no longer necessary for business operations
- **We must retain:** Information required for legal, tax, or regulatory compliance (typically 7 years for service records)
- **We may retain:** Anonymized data that cannot identify you

6.4 Right to Opt-Out

Marketing Communications: Unsubscribe from promotional emails, texts, or calls at any time through:

- "Unsubscribe" links in emails
- Replying "STOP" to text messages
- Contacting us directly

Service Communications: You cannot opt out of essential service communications (appointment confirmations, assessment results, payment notifications) while using our services.

6.5 Right to Data Portability

Request your data in a structured, commonly used format for:

- Transfer to another service provider
- Personal records
- Backup purposes

This right applies to data you provided to us and data we generated, where technically feasible to export.

6.6 Right to Restrict Processing

Request temporary restriction of data processing in specific situations:

- While disputing information accuracy
- When processing is unlawful but you prefer restriction over deletion
- When you need data for legal claims after we no longer need it
- While we verify legitimate grounds for processing you've objected to

6.7 Right to Object

Object to certain types of data processing:

- Marketing or promotional uses
- Profiling for marketing purposes
- Processing based on legitimate interests (we will cease unless we have compelling grounds)

6.8 Exercising Your Rights

How to Submit Requests:

- Email: privacy@alpaca-crew.com

- Mail: 548 Market Street, PMB 948619, San Francisco, CA 94104
- Phone: (510) 731-6110

What to Include:

- Your name and contact information
- Specific right you're exercising
- Relevant details to help us locate your information
- Preferred format for responses

Our Response Process:

- **Verification:** We may require identity verification to prevent fraudulent requests (typically government-issued ID or account verification)
- **Timeframe:** We respond within 30 days of receiving valid requests
- **Extensions:** Complex requests may require up to 60 additional days with notification
- **No Fee:** Most requests processed free of charge
- **Exceptions:** We may charge reasonable fees for excessive, repetitive, or manifestly unfounded requests

Appeal Rights: If you disagree with our response to a privacy request:

- Request internal review and reconsideration
- File complaints with relevant data protection authorities
- Pursue legal remedies as provided by applicable law

---

7. Cookies & Online Tracking

We use cookies and similar technologies to operate our website, improve functionality, analyze usage, and support service delivery.

This section explains what technologies we use, why we use them, how long they last, and how you can manage your preferences.

7.1 What Are Cookies and Tracking Technologies

Cookies are small data files placed on your browser or device when you visit our website. They allow us to recognize your browser, store preferences, and measure engagement. Related technologies include:

- **Web Beacons** – small transparent images used for analytics or email tracking;
- **Pixels or Tags** – code snippets that measure conversions or ad performance;
- **Local Storage** – browser-based data retention for faster page loading;
- **Session Tracking IDs** – temporary identifiers that maintain your active login; and

- **Device Fingerprinting** – used strictly for fraud prevention and not marketing.

We never use technologies designed to covertly collect personal or biometric information.

7.2 Categories of Cookies We Use

A. Essential Cookies

These are required for our site to function and cannot be disabled. They support:

- Secure login and authentication;
- Form submissions and booking requests;
- System load balancing and fraud prevention;
- Retaining service selections during checkout.
- Examples: Jobber session cookies, CSRF tokens, and secure payment cookies.

B. Performance and Analytics Cookies

- These help us understand how visitors interact with our website.
- Data collected is aggregated and anonymized whenever possible.
- We use analytics only to measure site performance, not for cross-site tracking.
- Examples: Google Analytics (anonymized IPs), Hotjar heatmaps (optional).

C. Functional Cookies

- Used to remember your preferences and enhance user experience.
- They may store information like language settings, region, or display preferences.
- Examples: “Remember Me” login tokens, chat widget settings.

D. Marketing and Referral Cookies

Used only when you give consent. These enable us to:

- Deliver relevant promotions about cleaning or assessment services;
- Track referral participation and service rewards;
- Measure the success of campaigns or partner links;
- Prevent duplicate referral credits.
- We do not use behavioral advertising or sell marketing cookie data to third parties.

7.3 Duration and Retention

- **Session Cookies** expire when you close your browser.
- **Persistent Cookies** last between 30 days and 12 months depending on purpose.

- **Local Storage Data** is retained until cleared manually or automatically after inactivity. All expiration periods comply with CCPA, CPRA, and GDPR data-minimization requirements.

7.4 Third-Party Cookie Disclosure

Some cookies are placed by our trusted service providers acting as data processors, including:

- Jobber (scheduling and client account management);
- Stripe and PayPal (payment verification);
- Google Cloud / AWS (content delivery and security);
- Twilio (client portal communications);
- Analytics partners under strict anonymization and non-retention agreements.

We review all third-party cookies annually to confirm necessity and compliance.

No third-party cookie may track you across unrelated websites.

7.5 Legal Basis and Consent (GDPR/CPRA Compliance)

We rely on the following legal bases for cookies:

- **Essential cookies** – legitimate interest in providing core functionality;
- **Analytics, functional, and marketing cookies** – your affirmative consent.

You can manage consent via our cookie banner, which appears upon first visit and anytime you clear cookies or reset preferences.

Your selections are stored securely and can be changed at any time.

We honor Global Privacy Control (GPC) and "Do Not Track" signals to the extent technically feasible.

7.6 How to Manage or Opt Out

You can manage cookie preferences by:

1. Adjusting settings via our on-site Cookie Preferences link or banner;
2. Sending an opt-out request to support@alpaca-crew.com;
3. Changing browser settings to block or delete cookies; or
4. Installing a GPC-enabled browser extension (https://globalprivacycontrol.org).

If you disable cookies, essential site features (booking forms, logins, or saved preferences) may not function properly, but you will still have access to general content.

7.7 Tracking Outside Our Website

alpaca-crew does not:

- Track visitors across third-party websites for advertising;
- Use retargeting networks or third-party behavioral profiling;
- Associate analytics identifiers with real-world identities; or
- Sell cookie data to advertisers or brokers.

Any cross-site data observed by analytics partners remains aggregated, pseudonymized, and time-limited.

7.8 Children's Privacy and Cookies

We do not knowingly use cookies to collect personal information from individuals under 16 years of age.

If we discover such data has been collected inadvertently, we will delete it immediately upon notice.

---

8. Data Retention

We retain personal and property-related information only as long as necessary to fulfill the purposes for which it was collected, meet legal and contractual obligations, resolve disputes, and maintain accurate business records.

Retention periods vary by data type, operational need, and applicable law.

8.1 General Retention Policy

All retention schedules are governed by:

- **Purpose limitation** – data is kept only for clearly defined uses.
- **Data minimization** – only the minimum amount necessary is retained.
- **Legal compliance** – records required by tax, labor, or regulatory laws are retained per statutory requirements.
- **Security integrity** – older records are securely archived, restricted, and eventually deleted or anonymized.

No data is stored indefinitely without lawful basis.

8.2 Retention by Category

A. Client and Service Records

Includes: client account data, contact information, service forms, invoices, communications, photos, and property assessments.

- **Retention Period:** 7 years after your last service date.
- **Purpose:** recordkeeping, dispute resolution, service verification, tax compliance.
- **Deletion:** secure deletion from all systems, backups, and archives within 90 days after expiration of the retention period.

B. Communications and Correspondence

Includes: client inquiries, support messages, and scheduling emails.

- **Retention Period:** 3 years after last communication.
- **Purpose:** quality control, training, and legal evidence in case of disputes.

C. Payment and Transactional Data

Includes: invoices, payment confirmations, and financial reconciliations.

- **Retention Period:** 7 years per IRS and California Franchise Tax Board requirements.
- **Storage:** encrypted, tokenized, and stored separately from other data categories.

D. Employee and Contractor Data

Includes: personnel files, payroll, tax forms, training records, and scheduling logs.

- **Retention Period:** during employment plus 7 years after separation.
- **Purpose:** labor-law compliance, insurance, and audit verification.
- **Destruction:** verified deletion with HR and payroll confirmation.

E. Property Photos and Visual Data

Includes: documentation collected during service visits (see Section 1.4).

- **Retention Period:** 7 years after last service, unless needed for legal or insurance purposes.
- **Deletion:** confirmed erasure from encrypted backups within 90 days.

F. AI-Generated and Anonymized Data

Includes: algorithmic insights, service statistics, and non-identifiable performance data.

- **Retention Period:** up to 10 years for research, system improvement, and audit purposes.
- **Safeguards:** all personal identifiers are permanently removed or obfuscated.
- **Reidentification Ban:** de-identified data is never re-linked to individuals.

G. Website, Analytics, and Cookie Data

Includes: session identifiers, device logs, and anonymized traffic data.

- **Retention Period:** 30 days to 12 months depending on purpose.
- **Purpose:** security monitoring, performance optimization, and fraud detection.

H. Legal, Insurance, and Compliance Records

Includes: claim investigations, regulatory filings, and policy acknowledgments.

- **Retention Period:** 7 years after closure or longer if mandated by law.
- **Storage:** encrypted and access-restricted to compliance personnel.

8.3 Inactive Accounts

- Accounts with no login or service activity for 3 consecutive years are marked inactive.
- Clients are notified 30 days before deletion.
- Upon deletion, essential records (e.g., invoices and insurance logs) may be retained for compliance.

After deletion, all access credentials, tokens, and stored preferences are revoked.

8.4 Deletion Requests

You may request deletion of eligible data at any time by emailing support@alpaca-crew.com.

We verify all deletion requests and confirm completion within 30 business days unless legal exceptions apply.

Deletion may be delayed or denied if retention is required for:

- Legal, tax, or contractual obligations;
- Security incident investigation;
- Enforcement of agreements; or
- Compliance with California or federal recordkeeping laws.

Where deletion is not possible, data will be de-identified and access restricted.

8.5 Deletion Verification and Backup Policy

After deletion, alpaca-crew conducts verification through:

- Secure overwrite of electronic files;
- Destruction certificates for physical documents;
- Audit logging of deletion events; and
- Confirmation to the requester (if applicable).

Deleted data may remain in encrypted backups for up to 90 days, after which backups are automatically purged.

8.6 Cross-Border Retention and Storage

If information is processed in multiple jurisdictions (e.g., by cloud providers in the U.S. or EU), we apply the most restrictive retention rule applicable to any relevant law.

Data stored outside the United States remains governed by this Privacy Policy and equivalent safeguards.

8.7 AI and Predictive Data Governance

AI-generated insights are subject to retention policies that:

- Limit training data lifespan to system relevance;
- Require encryption and pseudonymization;
- Restrict cross-model data reuse without new consent;
- Log AI access for audit and compliance oversight; and
- Ensure human review for all long-term model archives.

We never use client-identifiable data in future AI model training without express authorization.

8.8 Retention Review and Audit

All retention schedules are reviewed annually by the Compliance Officer to ensure alignment with evolving privacy laws, operational needs, and technological changes.

Changes are documented in our internal Data Inventory and Retention Register.

---

9. Communications & Consent

9.1 Text Messaging (SMS)

By providing your mobile phone number to alpaca-crew, you consent to receive text messages (SMS or MMS) related to scheduling, service updates, and account management.

We use SMS only for operational, informational, and transactional purposes—never for unsolicited marketing without your explicit written consent.

Purpose and Scope of SMS Communications

We send text messages strictly to:

- Confirm and remind you of scheduled cleaning or assessment appointments;
- Notify you of crew arrival or service completion;
- Provide updates on payment or invoice status;
- Communicate time-sensitive service adjustments or delays;
- Share referral or rewards updates (if enrolled); and
- Facilitate security verification or client account recovery.

We do not use SMS for promotional messages unless you have separately opted in to receive marketing texts.

Consent and Verification Requirements

By voluntarily providing your phone number and selecting SMS as a communication method:

- You give prior express consent to receive messages under TCPA (47 U.S.C. § 227).
- Consent may be obtained through digital form submission, recorded verbal confirmation, or written agreement.
- For promotional texts, we require "express written consent" as defined by TCPA and CTIA Messaging Principles.
- You may revoke consent at any time by replying "STOP" or by emailing support@alpaca-crew.com.

Consent is never a condition of purchasing or receiving services unless required for appointment coordination or safety notifications.

Message Frequency

Message frequency varies based on service activity, typically:

- 1–3 messages for scheduling confirmations and reminders;
- 1–2 messages per service visit for real-time updates;
- Occasional messages for follow-up or quality feedback.

Average range: 2–5 messages per appointment cycle**.**

We will not exceed reasonable frequency levels necessary for your service communication.

Carrier and Message Delivery Disclaimer

- Message and data rates may apply depending on your mobile plan.
- Carriers are not liable for delayed or undelivered messages.
- Delivery timing may vary based on network conditions or geographic coverage.
- Messages are transmitted through verified third-party providers (e.g., Twilio) under encryption and data-processing agreements.

Opt-Out and Assistance

To stop receiving SMS messages:

• Reply "STOP" to any alpaca-crew message to unsubscribe immediately.
• You will receive a one-time confirmation of your opt-out request.
• You may also email support@alpaca-crew.com or call (510) 731-6110 to revoke consent.

To request help or support, reply "HELP" to any text message, or email us directly.

Opt-outs are processed within one business day and confirmed in writing or by text.

Data Handling and Retention

SMS-related data—including message content, timestamps, delivery logs, and phone numbers—is retained only as long as necessary for:

- Service coordination and operational recordkeeping;
- Quality control and audit verification;
- Compliance with TCPA and record retention laws (typically 2 years); or
- Resolution of disputes or claim investigations.

All SMS logs are encrypted, access-restricted, and deleted after the retention period expires.

Third-Party Messaging Providers

We use Twilio or equivalent platforms to deliver messages securely and reliably.

Each provider operates under a written Data Processing Agreement (DPA) ensuring:

- Encryption in transit (TLS/SSL) and at rest (AES-256);
- Limited retention of delivery logs;
- No independent use or sale of client data; and
- Immediate deletion upon contract termination or client request.

We regularly review provider compliance and security certifications.

Opt-In for Marketing or Rewards Messages

If you opt into optional marketing or rewards communications, we will obtain separate, explicit written consent through:

- Web forms, SMS confirmation codes, or account portal settings;
- Documentation specifying that consent covers promotional and non-transactional content;
- Right to withdraw consent at any time via “STOP,” email, or your account settings.

You may still receive necessary service-related messages even if you opt out of marketing texts.

Privacy and Security

All text message data is treated as confidential communication under alpaca-crew’s Privacy Policy and applicable federal and state privacy laws.

We do not sell, rent, or disclose SMS contact data to unaffiliated third parties for marketing. All message content adheres to the CTIA Short Code Monitoring Handbook and carrier anti-spam standards.

Contact for SMS Privacy Requests

Email: support@alpaca-crew.com
Phone: (510) 731-6110
Subject Line: “SMS Privacy Inquiry”

We respond to all verified inquiries within 10 business days**.**

9.2 Email Communications

Service Emails: Account confirmations, appointment details, invoices, and service-related updates.

Marketing Emails: With consent, promotional content about services, special offers, and company updates.

Unsubscribe: Use "Unsubscribe" links in marketing emails. Service-related emails cannot be opted out while using our services.

9.3 Phone Communications

Call Recording: Phone calls with alpaca-crew may be recorded for quality assurance, training, and dispute resolution. You will be notified when calls are recorded.

Do Not Call: Marketing calls respect Do Not Call registry preferences. Service-related calls may still occur for active service coordination.

10. Special Categories

10.1 Commercial Clients

Additional Information Collected:

- Company names and business addresses
- Multiple contact persons within organization
- Service agreements and contract terms
- Business-specific service requirements
- Billing and accounting contact information

Business Use: Information used solely for service delivery, contract compliance, and business relationship management.

Additional Compliance: Commercial clients may have industry-specific compliance requirements addressed in separate data processing agreements.

10.2 Employee Information

alpaca-crew collects, uses, and safeguards employee and applicant information strictly for human-resources, payroll, compliance, and workplace-safety purposes.

All employment-related data is handled under this Privacy Policy, internal confidentiality agreements, and applicable labor and privacy laws.

Categories of Information Collected

We may collect the following types of employee and applicant information:

A. Identifiers and Contact Details

Name, address, email, phone number, emergency contacts, and government-issued identifiers (e.g., driver's license, SSN, EIN for contractors).

B. Employment and Payroll Data

Hiring forms, offer letters, job titles, compensation, time cards, scheduling logs, benefits enrollment, and tax withholding forms.

C. Compliance and Eligibility Records

I-9 verification documents, background checks (where permitted), proof of insurance, certifications, and safety-training records.

D. Performance and Training Information

Employee evaluations, quality-control scores, training completion records, and client-service feedback relevant to job duties.

E. Device and System Access Logs

Login credentials, system access timestamps, and role-based activity logs generated while using company devices or platforms.

F. Geolocation and Scheduling Data

For field staff, limited GPS or route data used only during working hours for job verification, dispatch efficiency, and safety monitoring.

G. Health and Safety Information

Injury reports, ergonomic or exposure assessments, and vaccination or medical-clearance documents if required by law.

H. Financial and Banking Information

Direct-deposit details, expense reimbursements, and payroll-related payment data.

Purpose of Collection and Use

Employee data is used exclusively to:

- Recruit, hire, and manage personnel;
- Administer payroll, benefits, and taxes;
- Comply with state and federal employment laws;
- Provide training and safety programs;
- Evaluate performance and quality of service;
- Coordinate scheduling and route management;
- Investigate misconduct, safety incidents, or policy violations; and
- Protect corporate assets and ensure workplace security.

We do not sell, trade, or share employee data for marketing or non-employment purposes.

Monitoring and Tracking Limitations

- Any electronic monitoring (e.g., GPS route tracking or login auditing) occurs only during active work hours and for legitimate business reasons.
- We do not record personal communications, off-duty activities, or non-work locations.
- Video or audio monitoring may occur only in designated workspaces and never in restrooms, break areas, or private spaces.

- All surveillance footage, if any, is retained for a limited time (typically 30–90 days) and deleted unless required for investigation.

Employees are informed before any monitoring technology is deployed.

Retention and Deletion Schedule

- Active employee records – retained during employment.
- Post-employment records – retained 7 years after separation to satisfy wage, tax, and insurance obligations.
- Recruitment data – retained 3 years after application or final contact.
- Health and safety records – retained 5 years or as required by OSHA.
- Access and security logs – retained 12 months unless needed for audit.

After these periods, all data is securely deleted or anonymized per Section 8 (Data Retention).

Employee Rights Under CPRA and Labor Law

Employees, applicants, and contractors have the right to:

- Know what personal information we collect, use, or disclose;
- Request access to their personnel file (Cal. Lab. Code §1198.5);
- Request correction of inaccurate records;
- Request deletion of personal data where legally permissible;
- Opt out of disclosure of sensitive identifiers not required for employment; and
- Receive non-retaliation for exercising these rights.

Requests may be submitted via support@alpaca-crew.com or in writing to HR.

We verify each request and respond within 45 days.

Third-Party HR Service Providers

We use trusted providers for HR, payroll, and benefits administration, such as:

- Payroll processors (e.g., ADP or QuickBooks Payroll);
- Insurance carriers and benefits administrators;
- Background-check vendors (for new hires, where authorized);
- Learning-management or training systems.

All operate under Data Processing Agreements requiring confidentiality, encryption, and compliance with CPRA and GDPR standards.

They are prohibited from retaining or using data for any purpose beyond contracted HR services.

Data Security and Access Controls

- All HR systems require multi-factor authentication and encrypted storage (AES-256).
- Access is role-based and limited to authorized HR and management personnel.
- Paper records are stored in locked facilities with restricted access.
- Employee data transmitted electronically is protected using TLS/SSL.
- Any breach involving HR data follows procedures in Section 5.4 (Data Breach Response).

Cross-Border Transfers and Remote Access

Where HR data is processed or stored in the United States or other jurisdictions, we ensure equivalent safeguards through:

- Standard Contractual Clauses (SCCs) for EU/UK employees or contractors;
- Data-minimization practices for remote HR system access;
- Confidentiality agreements for remote staff and administrators.

Employee Training and Confidentiality

All employees with access to personnel information must complete annual privacy and data-protection training.

Confidentiality obligations survive termination of employment.

Contact for Employee Privacy Inquiries

Email: support@alpaca-crew.com
Phone: (510) 731-6110
Subject Line: "Employee Privacy Request"

We respond to verified HR privacy inquiries within 30 business days and maintain documentation of all requests and resolutions.

10.3 Children's Privacy

Our services are not intended for individuals under 13 years of age.

No Knowing Collection: We do not knowingly collect information from children under 13.

Discovery & Deletion: If we discover we have collected such information, we will delete it immediately.

Parental Rights: Parents or guardians may contact us to review, modify, or delete any child information inadvertently collected.

11. Client-Controlled Systems

11.1 Surveillance & Security Systems

Client Responsibility: Many properties have security cameras, alarm systems, or other monitoring devices controlled by clients.

Staff Awareness: Our employees are informed when surveillance systems are present and understand they may be recorded during service.

No alpaca-crew Access: alpaca-crew does not access, control, view, record, or use any footage or data from client-controlled surveillance systems. Our AI does not process surveillance footage.

Staff Privacy Rights: Our employees have privacy expectations and should be notified of surveillance systems that may record them.

Footage Use: Any use of surveillance footage for disputes, complaints, or legal matters remains under client control. We may request footage when investigating service issues.

11.2 Smart Home Systems

Properties may contain smart home devices (voice assistants, smart thermostats, connected appliances):

- We do not access or control these devices
- Our staff may need to interact with devices for service delivery (adjusting thermostats, etc.)
- Clients should review their device privacy settings and data collection practices
- We are not responsible for data collected by client-controlled smart devices

---

12. Third-Party Services & Links

12.1 External Links

Our website may contain links to external websites, contractor websites, or other service providers.

No Control: We do not control external sites and are not responsible for their:

- Privacy practices
- Content accuracy

- Security measures
- Data collection methods

Your Responsibility: Review privacy policies of external sites before providing personal information.

12.2 Third-Party Service Providers

We use third-party services for our operations:

- **Jobber:** Scheduling and billing platform
- **Payment processing:** Stripe, PayPal, etc.
- **Website analytics:** Google Analytics
- **Communication platforms:** Email, SMS services
- **Cloud storage and hosting**

Their Policies: These providers have their own privacy policies governing data they collect and process.

Our Vetting: We select reputable providers but cannot guarantee their practices or be responsible for their data handling.

---

13. International Data Transfers

alpaca-crew operates primarily in the United States but may process or store information in other jurisdictions where our service providers or cloud infrastructure operate.

When your data is transferred internationally, we ensure it receives an equivalent level of protection as required by applicable privacy laws, regardless of where processing occurs.

13.1 When International Transfers Occur

We may transfer personal data:

- To our cloud hosting providers (e.g., AWS, Google Cloud) that maintain global data centers for redundancy and uptime;
- To service providers or AI-processing partners that perform data analysis or platform maintenance outside your home jurisdiction;
- When a client, contractor, or referred partner operates internationally; or
- For backup, technical support, or secure storage in another region.

Such transfers occur only when necessary for operational continuity, legal compliance, or requested services.

13.2 Legal Basis for Transfers

Depending on your location and applicable law, we rely on one or more of the following mechanisms:

A. Adequacy Decisions

Transfers to countries officially recognized by the European Commission, UK ICO, or California Privacy Protection Agency (CPPA) as providing adequate data protection (e.g., the EU–U.S. Data Privacy Framework).

B. Standard Contractual Clauses (SCCs)

Where adequacy decisions do not apply, we execute Standard Contractual Clauses (SCCs) adopted by the European Commission (2021/914/EU) or the UK's International Data Transfer Addendum, ensuring equivalent obligations for confidentiality, security, and data subject rights.

C. Binding Corporate Rules (BCRs)

If applicable, transfers within corporate affiliates or long-term service providers may be governed by approved BCRs validated by relevant supervisory authorities.

D. Consent and Contractual Necessity

For one-time or client-initiated transfers (e.g., communicating with a contractor in another country), we rely on explicit consent or necessity for service performance.

13.3 Safeguards and Oversight

To protect transferred data, alpaca-crew and its providers implement:

- **Encryption in transit and at rest** for all international transfers (TLS/SSL, AES-256);
- **Access controls** restricted to authorized personnel on a least-privilege basis;
- **Audit trails** recording each transfer event and recipient system;
- **Data minimization** – only essential fields are transmitted;
- **Transfer Impact Assessments (TIAs)** evaluating destination risk, surveillance exposure, and vendor compliance;
- **Annual certification review** for all vendors engaged in cross-border processing.

All third parties are required by written contract to handle data in accordance with this policy and relevant laws.

13.4 Your Rights Regarding International Transfers

You have the right to:

- Request information about where your data is stored or processed;
- Obtain a copy of the relevant transfer mechanism (e.g., SCCs or adequacy decision summary);
- Object to transfers based on compelling privacy or safety grounds; and
- Request deletion or restriction of your data if cross-border storage is no longer necessary.

Requests should be sent to support@alpaca-crew.com with the subject line "International Data Transfer Inquiry."

Verified responses are provided within 45 days, extendable under law.

13.5 Cross-Border Vendor Accountability

We ensure all international service providers:

- Operate under binding confidentiality and data-processing agreements;
- Provide ongoing proof of compliance (SOC 2 Type II, ISO 27001, or similar);
- Undergo periodic reviews and risk assessments; and
- Notify alpaca-crew within 72 hours of any suspected incident affecting transferred data.

Vendors that fail to maintain adequate protection are suspended or terminated.

13.6 Law-Enforcement and Government Requests

If a foreign government or law-enforcement authority requests access to your data, alpaca-crew:

1. Evaluates the request for legal validity and proportionality;
2. Notifies you unless legally prohibited; and
3. Limits disclosure strictly to the extent required by law.

We never voluntarily provide bulk or unrestricted access to personal data.

13.7 Data Residency and Backup Regions

- Primary storage: United States (California and Oregon data centers).
- Backup and redundancy: May include encrypted servers in Canada or the EU for system stability.
- Retention: governed by Section 8 (Data Retention) and deleted upon expiration or verified request.

All replicas and backups remain subject to the same technical and contractual safeguards as the original data.

13.8 International Cooperation and Compliance

alpaca-crew cooperates with relevant data-protection authorities to resolve cross-border data inquiries.

If any transfer mechanism becomes invalid or replaced under law, we will promptly update our contractual safeguards and notify affected clients through this policy or direct notice.

---

14. Legal Basis for Processing (GDPR & Similar Laws)

For individuals in jurisdictions with comprehensive privacy laws (EU, UK, California, etc.), we process personal data based on:

14.1 Contract Performance

Processing necessary to provide services you've requested, including:

- Scheduling and coordinating services
- Processing payments
- Providing assessment reports
- Managing your account

14.2 Legitimate Interests

Processing necessary for our legitimate business interests, including:

- Service improvement and quality assurance
- Fraud prevention and security
- Business analytics and planning
- Employee management and coordination
- Marketing to existing clients (where permitted)
- AI system development and improvement

We balance these interests against your privacy rights and do not process data where your interests override ours.

14.3 Legal Obligations

Processing required to comply with legal requirements:

- Tax and accounting obligations
- Regulatory reporting
- Legal process and court orders

- Employment law compliance

14.4 Consent

Processing based on your explicit consent for:

- Marketing communications
- Optional data sharing with specific third parties
- Non-essential cookies and tracking
- Optional AI analysis features

You may withdraw consent at any time without affecting the lawfulness of processing before withdrawal.

14.5 Legitimate Interest Assessments

We regularly assess whether our legitimate interests are balanced against your privacy rights. You may request information about specific legitimate interest assessments.

---

15. Automated Decision-Making

15.1 AI Assessments

Our AI systems make automated assessments about property conditions, but these do not constitute automated decision-making that significantly affects you because:

- All AI reports undergo human review before delivery
- AI recommendations require your explicit approval before implementation
- You maintain complete control over service decisions
- AI analysis is one input among many for decision-making

15.2 No Harmful Profiling

We do not engage in:

- Automated profiling for discriminatory purposes
- Automated decisions that significantly affect legal rights or services without human involvement
- High-risk automated decision-making without safeguards

15.3 Right to Human Review

You have the right to:

- Request human review of any automated assessments
- Understand the logic behind automated decisions
- Challenge automated recommendations
- Receive explanations of AI-generated content

15.4 Human Review Rights (AI-Related)

alpaca-crew integrates artificial intelligence ("AI") and automated systems to assist in generating property assessments, cleaning recommendations, and maintenance insights.

These tools enhance consistency, accuracy, and efficiency but do not replace human judgment or professional evaluation**.**

All AI-generated assessments are reviewed by qualified personnel before final delivery.

Purpose of AI Use

AI systems are used solely to:

- Analyze structured service data, property photos, and form submissions;
- Generate maintenance or cleaning recommendations;
- Classify service tiers and surface conditions;
- Identify recurring issues or efficiency trends; and
- Support internal quality assurance and reporting.

AI is not used to make independent contractual, financial, or legal decisions about clients, employees, or contractors.

Human Oversight and Accountability

- Every AI-generated report or recommendation is reviewed, validated, and approved by an alpaca-crew assessor or manager before being sent to the client.
- Human reviewers may modify, reject, or supplement AI conclusions to ensure factual accuracy and professional relevance.
- No service price, classification, or referral is finalized without human confirmation.
- We document all review actions to ensure transparency and accountability.

Our AI models assist humans—they do not autonomously determine eligibility, pricing, or service outcomes.

Accuracy, Bias, and Quality Controls

We actively monitor AI outputs to reduce bias, ensure fairness, and maintain report quality through:

- Regular audits of model accuracy and error rates;
- Validation of training datasets to prevent inclusion of sensitive or biased information;
- Human quality assurance comparing AI recommendations against real-world outcomes;
- Internal review panels that oversee AI performance and policy compliance.

If a material inaccuracy or bias is detected, we promptly correct affected reports and retrain the model as necessary.

Client Rights Regarding AI-Generated Information

Under applicable privacy and data-protection laws, you have the right to:

- **Know** when AI or automated systems are used in your report;
- **Access** and review the logic or factors influencing AI-based recommendations;
- **Request human review** of any AI-generated conclusion that may affect your service, pricing, or property evaluation;
- **Request correction or clarification** of inaccurate or misleading AI outputs;
- **Obtain a plain-language explanation** of the data and methodology used; and
- **Withdraw consent** for continued use of your data in AI model training.

Requests can be submitted to support@alpaca-crew.com with the subject line "AI Human Review Request." Verified responses are provided within 45 days unless additional time is needed under law.

Limitations and Disclaimers

- AI insights are advisory only and do not constitute engineering, structural, or professional maintenance evaluations.
- AI recommendations are based on observed or submitted data and may not reflect hidden or evolving property conditions.
- alpaca-crew is not responsible for third-party use or interpretation of AI reports outside authorized contexts.
- Clients are encouraged to verify significant recommendations with licensed professionals.

Our responsibility is limited to the accuracy of data processed and the quality of human-verified reports.

Training Data and Privacy Protection

AI models may be trained on de-identified and anonymized datasets derived from service reports, aggregated property conditions, and non-personal metrics.

We ensure:

- All identifiers are permanently removed before training;

- Training data is never re-linked to individual clients or locations;
- Use of your data for AI improvement is opt-in only under Section 0.3 (Your Privacy Choices)**;** and
- You may request deletion or exclusion of your anonymized data from future model updates.

Transparency and Future Disclosures

As AI laws evolve, alpaca-crew will update this section to reflect new disclosure and accountability standards.

Clients will be notified of material updates through website notices or direct email communication.

We continuously review all AI systems to ensure fairness, explainability, and compliance with privacy and consumer-protection laws.

---

16. Privacy Policy Limitations

While alpaca-crew takes extensive measures to protect your personal and property information, no system is completely immune from risk.

This section outlines the legal, operational, and jurisdictional boundaries of our privacy commitments.

16.1. Reasonable-Measures Standard

We implement administrative, technical, and physical safeguards consistent with industry standards—encryption, access controls, employee training, and vendor oversight—to maintain confidentiality, integrity, and availability of data.

However, absolute security cannot be guaranteed. By using our services, you acknowledge and accept the inherent risks associated with electronic data transmission and storage.

16.2. Events Beyond Our Control (Force Majeure)

We are not responsible for loss, delay, or disclosure of information caused by events beyond our reasonable control, including but not limited to:

- Cyber-attacks, system failures, or Internet outages;
- Acts of nature (fire, flood, earthquake);
- War, terrorism, civil unrest, or government action;
- Power failures or telecommunication disruptions; or
- Vendor or carrier outages outside our direct control.

In such circumstances, we will act promptly to restore operations and notify affected clients when legally required.

16.3. Third-Party Data Handling and Referrals

Once information is voluntarily shared with independent third parties—such as referred contractors, insurance providers, or external service platforms—alpaca-crew cannot control how those entities use, store, or protect it.

We require reasonable assurances of compliance through written agreements but cannot guarantee their performance.

Clients are encouraged to review third-party privacy policies before engaging their services. alpaca-crew is not liable for damages, misuse, or breaches occurring after data leaves our direct control, except where required by law.

16.4. Legal and Regulatory Exceptions

This Privacy Policy does not restrict disclosures that are:

- Required by law, subpoena, or regulatory investigation;
- Necessary to detect, prevent, or respond to fraud or security incidents;
- Needed to protect health, safety, or property in an emergency; or
- Permitted under CPRA and similar privacy laws for lawful business purposes.

Where feasible, we will notify affected individuals before such disclosure unless prohibited by law or court order.

16.5. Jurisdiction and Cross-Border Limitations

Our services are primarily intended for users in the United States.

International clients acknowledge that data processed in the U.S. may be subject to U.S. laws and lawful access requests.

We apply equivalent safeguards under Section 13 (International Data Transfers) but cannot ensure identical privacy regimes across jurisdictions.

16.6. Accuracy of Information and Client Responsibilities

We rely on clients, contractors, and partners to provide accurate, up-to-date information.

We are not responsible for errors or delays resulting from incomplete, false, or outdated data. Clients should promptly update account or contact information to ensure proper service and compliance.

16.7. No Waiver of Legal Rights

Nothing in this policy limits rights provided under applicable privacy, consumer-protection, or employment laws.

However, alpaca-crew's maximum liability for privacy-related claims shall not exceed the total amount paid for services during the preceding 12 months, except as otherwise required by statute.

16.8. Policy Updates and Material Changes

We may revise this Privacy Policy as technology, regulations, or business practices evolve.

Significant updates will be communicated via email or website notice at least 30 days before the effective date.

Continued use of our services after notice constitutes acceptance of the updated terms.

16.9. Contact and Escalation of Concerns

Questions or concerns regarding these limitations may be directed to:

Email: support@alpaca-crew.com
Phone: (510) 731-6110
Mail: 548 Market Street, PMB 948619, San Francisco, CA 94104

Unresolved privacy issues may also be submitted to the California Privacy Protection Agency (CPPA) or the appropriate consumer-protection authority in your jurisdiction.

---

17. Changes to This Privacy Policy

17.1 Right to Modify

We may update this Privacy Policy to reflect:

- Changes in business practices
- New legal or regulatory requirements
- Improvements in privacy protections
- Technological developments

17.2 Notice of Changes

Effective Date: Updates become effective immediately upon posting to our website with updated "Last Updated" date.

Material Changes: For significant changes affecting how we handle personal information, we will provide additional notice through:

- Email to address on file
- Prominent website notification
- In-app notifications if applicable

Your Responsibility: Review this policy periodically to stay informed of changes.

17.3 Continued Use

Continued use of our services after policy updates constitutes acceptance of revised terms.

17.4 Version History

We maintain version history of our Privacy Policy and can provide previous versions upon request for reference or legal purposes.

---

18. Contact Information & Data Protection

18.1 Privacy Inquiries

For questions about this Privacy Policy or to exercise privacy rights:

Email: privacy@alpaca-crew.com
Mail: 548 Market Street, PMB 948619, San Francisco, CA 94104
Phone: (510) 731-6110

18.2 Data Protection Officer

For jurisdictions requiring a Data Protection Officer, contact information is available upon request.

18.3 Response Timeframe

We respond to privacy inquiries within:

- Initial acknowledgment: 5 business days
- Full response: 30 days for most requests

- Complex requests: Up to 60 additional days with notification

18.4 Supervisory Authority

If you believe we have not adequately addressed your privacy concerns, you have the right to lodge a complaint with relevant data protection authorities in your jurisdiction.
