Unified Metrics

COMPREHENSIVE PRIVACY POLICY

UNIFIED SOLUTION SERVICES CORP · Version 1.0 · Effective October 1, 2026 · Issued 10/1/2026, 5:54:14 AM

Unified Metrics Comprehensive Privacy Policy

Effective Date: October 1, 2026

Last Updated: October 1, 2026

This Comprehensive Privacy Policy (Privacy Policy) describes how UNIFIED SOLUTION SERVICES CORP, doing business as Unified Metrics (Unified Metrics, we, us, or our), collects, uses, protects, discloses, retains, and transfers personal information through the Unified Metrics software platform, mobile applications, web portals, cloud services, and related sites (collectively, the Service).

This Privacy Policy applies to business owners, general contractors, specialty trade contractors, independent subcontractors, construction crew members, employees, clients, and visitors who access or interact with the Service.

Please read this Privacy Policy carefully. By creating an account, accessing our applications, or using any part of the Service, you acknowledge that you have read, understood, and agree to the practices described herein. If you do not agree with this Privacy Policy, you must immediately discontinue use of the Service.

1. SCOPE, DUAL-WORKSPACE ARCHITECTURE & ROLES

1.1 Enterprise multi-tenancy & strict partition

Unified Metrics operates a multi-tenant business operating system featuring strict multi-workspace isolation:

Business Workspace: Designed for commercial construction accounting, project costing, crew scheduling, daily logs, client invoicing, contractor records, and business tax preparation. In this workspace, your company acts as the Data Controller (or "Business" under applicable state privacy laws) regarding workforce, vendor, and customer records.

Personal Workspace: A completely distinct, segregated environment for personal household budgeting, personal tax preparation (e.g., Form 1040 Schedules, Schedule C/SE records), and personal expense vaults. Data stored in your Personal Workspace is never commingled, shared with, or accessible by your employer, general contractor, or Business Workspace colleagues.

1.2 Our role as Service Provider vs. Business

Under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, CCPA/CPRA), and other applicable U.S. state privacy laws:

When we process employee, subcontractor, client, or job site data strictly on behalf of an enterprise customer pursuant to our Master Terms of Service, we act as a Service Provider or Processor.

When we collect information directly from individual account holders for account registration, billing, security authentication, direct marketing, or within a self-managed Personal Workspace, we act as a Business or Controller.

2. CATEGORIES OF PERSONAL INFORMATION WE COLLECT

We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device (Personal Information).

Within the past twelve (12) months, we have collected the following statutory categories of Personal Information:

Statutory CategorySpecific Data Elements CollectedCollected For

A. IdentifiersReal name, business alias, signature, postal address, business address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, telephone number, account username, and password hashes.Identity verification, account administration, customer communication, multi-tenant authentication, and security logging.

B. Personal Records (Cal. Civ. Code § 1798.80(e))Legal name, business registration state, telephone number, bank account details (for payouts via payment processors), credit/debit card numbers (tokenized by PCI-compliant payment gateways), employment status, trade certifications, and insurance policy details.Invoicing, subscription billing, contractor tax summaries, and credential verification.

C. Protected Classifications & Government IDs (Sensitive Personal Information)Federal Employer Identification Numbers (FEIN), Social Security Numbers (SSN), or Individual Taxpayer Identification Numbers (ITIN) collected strictly via official Form W-9 uploads or contractor tax prep workflows.Mandatory U.S. tax compliance, 1099-NEC/1099-MISC preparation, and audit trails.

D. Commercial InformationRecords of services estimated, contracted values, invoices sent/received, expense categorizations, material receipts, change orders, project milestones, payout logs, and subscription tier history.Core functionality of project accounting, estimate generation, job costing, and financial reporting.

E. Internet or Network ActivityBrowser type, operating system version, app version, device hardware specifications, access timestamps, pages viewed, user journey clicks, error stack traces, and API request latency logs.Application diagnostics, infrastructure optimization, bug fixing, and intrusion detection.

F. Geolocation DataApproximate location derived from IP address; precise physical location (latitude/longitude coordinates) collected solely when you explicitly grant device permissions during mobile check-ins, job site arrival verifications, or field photo captures.Verifying job site presence, geofencing daily job logs, and timecard auditability.

G. Audio, Electronic, Visual InformationJob site progress photographs, material delivery photos, receipt capture camera snapshots, voice notes submitted for transcriptions, and customer support ticket attachments.Daily construction documentation, optical character recognition (OCR) receipt parsing, dispute resolution, and audit defense.

H. Professional or Employment InformationJob titles, construction trade/specialty (e.g., Framing, Roofing, Electrical, HVAC, Plumbing), hourly billing rates, piecework unit rates, contractor license numbers, worker compensation coverage status, and company association history.Labor costing, sub-tier contractor management, crew dispatching, and field communication.

I. Inferences Drawn from DataProjected completion margins, labor productivity ratios, planned vs. actual material expense variances, budget burn-rates, and predictive job-costing forecasts.AI-driven insights, proactive variance alerts, and executive financial summaries.

Personal Information does not include publicly available government records, de-identified or aggregated consumer information, or information excluded from state privacy laws (such as health data governed by HIPAA or financial data covered by GLBA).

---

3. SOURCES FROM WHICH WE COLLECT INFORMATION

We collect the categories of Personal Information listed above from the following distinct sources:

Directly from You: Information you submit when registering an account, creating estimates, scanning physical receipts, uploading Form W-9s, logging daily site notes, requesting customer support, or filling out your business and personal tax profiles.

From Your Employer, General Contractor, or Project Owner: If you access the Service as an employee or invited subcontractor, the primary business tenant may input your name, contact details, trade rates, and project assignments to manage field operations.

Automated Technologies & Device Telemetry: When you interact with our web platform or mobile applications, our servers automatically log connection data, device characteristics, cookies, and local storage tokens necessary for session persistence.

Camera & Device Sensors (With Explicit Authorization): When you take a photo of a material receipt or job site condition, our app requests explicit runtime permission to access your camera, photo gallery, or device GPS. You may revoke these permissions at any time via your device settings.

Integrated Payment & Banking Partners: When you pay for subscriptions or process project invoices, our third-party payment gateways (e.g., Stripe) return secure verification tokens, transaction IDs, and card brand/last 4 digits. We never receive or store raw credit card numbers, CVVs, or full bank account credentials on our servers.

---

4. BUSINESS AND COMMERCIAL PURPOSES FOR DATA USE

Unified Metrics uses your Personal Information strictly for legitimate commercial and business purposes:

4.1 Delivering and maintaining the Service

Facilitating the creation, calculation, and delivery of construction estimates, invoices, and change orders.

Providing job costing, daily logs, field issue tracking, and multi-party crew coordination.

Executing automated financial summaries, labor allocations, and material tracking.

Maintaining separate data vaults for Business and Personal accounts.

4.2 Security, Fraud Prevention, and Identity Verification

Verifying user identity, credentials, and multi-factor authentication codes.

Enforcing role-based access controls (Owner, Admin, Manager, Employee, Worker).

Protecting the integrity, confidentiality, and availability of multi-tenant databases.

Detecting, investigating, and preventing unauthorized access, security incidents, or fraudulent use.

4.3 Tax Documentation and Compliance Workflows

Storing and rendering encrypted Form W-9s and contractor tax summaries.

Assisting users in tracking 1099-NEC contractor payout thresholds ($600 federal informational threshold).

Providing educational IRS form templates (e.g., Form 1040-ES, Schedule C, Schedule SE).

Ensuring that sensitive tax numbers (SSN/FEIN) are only displayed with masked previews and strict audit-logged reveals.

4.4 Product Improvement, Analytics, and Customer Support

Diagnosing technical errors, database latency, and system outages.

Responding to customer inquiries, support tickets, and bug reports.

Developing performance optimizations, UI improvements, and new operational features.

---

5. ARTIFICIAL INTELLIGENCE (CHLOE) & DATA PROCESSING BOUNDARIES

Unified Metrics integrates an internal artificial intelligence layer (Chloe) designed as a silent, executive financial analyst. We adhere to the following strict operational boundaries:

5.1 Strictly Read-Only for Financial Data

Chloe operates as an informational and consultative tool. Chloe cannot execute financial transactions, alter accounting ledgers, modify invoice totals, or write data to your business or personal database without explicit, manual user review and confirmation.

5.2 Proprietary Shielding & No Third-Party Model Training

When Chloe analyzes an estimate, project variance, or receipt OCR payload, your query is processed securely through enterprise AI gateways.

We do not sell, rent, or permit our third-party AI model providers to use your confidential business data, financial records, client names, or Personal Information to train, refine, or improve their general machine learning or foundation models.

Data transmissions to enterprise AI gateways are stateless, encrypted in transit, and governed by strict zero-data-retention or commercial enterprise privacy terms.

5.3 User Discretion and Verification

AI-generated forecasts, expense classifications, and risk analyses are estimates provided for convenience only. You maintain full professional responsibility for verifying all numbers, tax calculations, and contract documents before relying on or distributing them.

---

6. DISCLOSURES AND SHARING OF PERSONAL INFORMATION

6.1 Strict "No Sale" and "No Cross-Context Behavioral Advertising" Commitment

Unified Metrics does NOT sell your Personal Information.

Unified Metrics does NOT share your Personal Information with third parties for cross-context behavioral advertising, targeted advertising, or commercial data brokering. We have not engaged in such sales or shares in the preceding twelve (12) months.

6.2 Disclosures for Business Purposes

We disclose Personal Information only to trusted service providers, partners, and authorized users under the following defined circumstances:

Authorized Workspace Collaborators: Your project estimates, time entries, daily logs, and trade contact information are visible to authorized members of your companys workspace according to role permissions assigned by your company administrator.

Explicit Consent-Driven Contractor W-9 Sharing: When a General Contractor connects with an Independent Subcontractor via Public ID, no tax document or sensitive tax identifier is shared automatically. Form W-9 files are transferred to the requesting business vault only after the Subcontractor receives a specific, independent prompt and grants explicit, affirmative consent. Every transfer is permanently timestamped and recorded in our immutable audit log.

Third-Party Service Providers (Subprocessors): We share data with verified third-party vendors who provide essential infrastructure services under strict contractual confidentiality and data protection terms:

Cloud Hosting & Database Storage: Distributed enterprise cloud storage providers utilizing hardware-level encryption (AES-256) and automated replication.

Payment Processors: PCI-DSS Level 1 certified processors managing subscription billing and customer invoice payouts.

Transactional Communications Providers: Email and SMS delivery gateways executing two-factor authentication, account alerts, and system notices.

Document Parsing & OCR Engines: Ephemeral image processing engines extracting vendor names, dates, and currency totals from receipt captures.

Legal Compliance and Lawful Requests: We may disclose your information if required to do so by applicable federal or state law, valid subpoena, court order, or official government audit, provided that we make reasonable efforts to notify you in advance unless prohibited by law or court order.

Business Transfers: If Unified Metrics undergoes a merger, acquisition, corporate reorganization, asset sale, or bankruptcy, your information may be transferred to the acquiring entity as part of the transaction, subject to the protections of this Privacy Policy.

---

7. DATA RETENTION & DESTRUCTION SCHEDULE

We retain Personal Information only for as long as reasonably necessary to fulfill the purposes for which it was collected, satisfy our legal, accounting, and reporting obligations, and resolve ongoing contractual disputes.

7.1 Specific Retention Timelines

Data CategoryActive Account RetentionPost-Account Termination RetentionStatutory Justification

Financial Ledgers, Invoices & EstimatesRetained continuously while the account is active.Retained for seven (7) years following the calendar year of account closure.Compliance with Internal Revenue Service (IRS) regulations, state tax auditing standards, and Florida statutory contract limitation periods.

Form W-9 & Tax Vault DocumentsRetained continuously until replaced or revoked by the user.Retained for seven (7) years from the date of the last financial transaction referencing the taxpayer.IRS Form 1099 compliance, audit defense, and federal backup withholding regulations.

Daily Site Logs & Job PhotosRetained continuously while workspace is active.Retained for up to four (4) years post-project closure or account termination, unless earlier purged by the Owner.Construction defect statutes of limitation (Florida Stat. § 95.11) and insurance claim substantiation.

User Authentication & Log TelemetryRolling 90-day retention for routine connection logs.Deleted within 180 days of account termination, except security incident logs retained up to two (2) years.System security audits, fraud defense, and brute-force intrusion analysis.

Personal Workspace DataRetained strictly at the sole discretion of the individual user.Irrevocably purged within thirty (30) days of an explicit account deletion request.Consumer privacy autonomy and strict separation from commercial accounts.

7.2 Secure Destruction Protocols

Upon the expiration of the applicable retention period or upon verified consumer deletion request, data is permanently expunged using cryptographically secure wiping protocols, multi-pass physical drive overwriting, or complete logical block de-allocation across all distributed production and backup clusters.

---

8. CALIFORNIA CONSUMER PRIVACY RIGHTS (CCPA / CPRA NOTICE)

If you are a resident of California, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (CCPA/CPRA), grants you specific statutory rights regarding your Personal Information:

8.1 Right to Know / Access

You have the right to request that we disclose to you:

The categories of Personal Information we have collected about you.

The categories of sources from which the Personal Information was collected.

The business or commercial purpose for collecting your Personal Information.

The categories of third parties to whom we disclose that Personal Information.

The specific pieces of Personal Information we have collected about you (data portability).

8.2 Right to Request Deletion

You have the right to request that we delete Personal Information that we have collected directly from you, subject to statutory exceptions (such as our legal obligation to retain financial transaction records under federal or Florida tax laws, detect security incidents, or protect against fraudulent conduct).

8.3 Right to Correct Inaccurate Personal Information

You have the right to request that we rectify inaccurate, outdated, or incomplete Personal Information maintained about you in our active records.

8.4 Right to Opt-Out of the Sale or Sharing of Personal Information

Because Unified Metrics does not sell or share Personal Information for cross-context behavioral advertising, we do not provide a "Do Not Sell or Share My Personal Information" opt-out link.

8.5 Right to Limit Use and Disclosure of Sensitive Personal Information

We collect Sensitive Personal Information (such as SSNs, FEINs, and precise geolocation) strictly to provide the core services requested by you (e.g., generating required tax filings, verifying job site check-ins) or as authorized by California law. We do not use or disclose Sensitive Personal Information for purposes other than those specified in Cal. Civ. Code § 1798.121 and its implementing regulations.

8.6 Right to Non-Discrimination

We will not discriminate against you for exercising any of your CCPA/CPRA rights. We will not deny you goods or services, charge you different prices or rates, or provide a different quality of service because you exercised your statutory privacy rights.

8.7 Exercising Your California Privacy Rights

To submit a verifiable consumer request to know, delete, or correct your Personal Information:

Email: Send an email to contact@unifiedsolutionsgroup.co with the subject line "California Privacy Rights Request".

In-App Portal: Navigate to Settings > Legal & Compliance > Submit Privacy Request.

Verification Procedure: To protect your security and privacy, we must verify your identity before processing your request. We will match the identifying information provided in your request (such as your account email, business phone number, and recent transaction timestamp) against the information maintained in our database. If you maintain a password-protected account, we may verify your identity through your existing login session.

Authorized Agents: You may designate an authorized agent registered with the California Secretary of State to submit requests on your behalf. We will require written proof of the agents authorization and will verify your identity directly with you.

8.8 California Shine the Light Law (Cal. Civ. Code § 1798.83)

California residents are entitled once a year, free of charge, to request and obtain certain information regarding our disclosure, if any, of personal information to third parties for their direct marketing purposes in the preceding calendar year. Unified Metrics does not disclose personal information to third parties for their direct marketing purposes.

---

9. RIGHTS UNDER OTHER U.S. STATE PRIVACY LAWS

Residents of Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), Texas (TDPSA), and other states with comprehensive consumer privacy statutes enjoy similar rights regarding access, correction, deletion, and data portability.

If you reside in one of these jurisdictions, you may exercise your rights through the same channels described in Section 8.7. If we decline to take action on your request, you have the right to appeal our decision by contacting us at contact@unifiedsolutionsgroup.co with the subject line "Privacy Request Appeal." We will respond to your appeal within the statutory timeframe mandated by your states law.

---

10. ELECTRONIC COMMUNICATIONS & TCPA COMPLIANCE CONSENT

10.1 Service-Related Transactional Communications

By registering an account with Unified Metrics, you agree that we may send you mandatory electronic communications regarding your account, including:

Two-factor authentication (2FA) codes and password reset instructions.

Billing statements, payment receipts, and subscription renewal notices.

Project notifications, change order approvals, and crew dispatch assignments.

Critical security alerts, terms updates, and service interruption advisories.

These transactional messages are required for the proper administration of the Service, and you cannot opt out of receiving them while your account remains active.

10.2 SMS / Text Messaging Consent (TCPA Notice)

Where you provide your mobile telephone number and expressly opt in to receive SMS alerts:

Consent: You grant Unified Metrics and its automated messaging systems express consent under the Telephone Consumer Protection Act (47 U.S.C. § 227) (TCPA) to transmit operational text messages, job site status alerts, and multi-factor security verification codes to the provided number.

Non-Condition of Purchase: Providing SMS consent is not a condition of purchasing any paid subscription, software license, or product.

Message & Data Rates: Standard message and data rates applied by your wireless carrier may apply to all incoming and outgoing text messages.

Opt-Out Procedure: You may revoke your SMS consent at any time by replying STOP to any text message received from our system, or by disabling SMS notifications within Settings > Phone Alerts. For help, reply HELP or contact customer support.

10.3 Marketing Communications & Opt-Out

We may occasionally send you promotional emails regarding new features, educational webinars, or platform upgrades. You can opt out of marketing emails at any time by clicking the Unsubscribe link at the bottom of any marketing email or by updating your preferences in Settings > Notifications. Opting out of marketing emails does not affect transactional or legal service notices.

---

11. DATA SECURITY & STORAGE ARCHITECTURE

We implement rigorous administrative, technical, and physical safeguards designed to protect Personal Information from unauthorized access, destruction, loss, alteration, or disclosure:

Encryption In-Transit: All network traffic between your client device and our servers is secured using modern Transport Layer Security protocols (TLS 1.3 / TLS 1.2) with forward secrecy.

Encryption At-Rest: Databases, backups, file vaults, and stored document assets are encrypted at rest using industry-standard AES-256 encryption algorithms.

Row-Level Security (RLS): Our multi-tenant database enforces programmatic, database-level Row-Level Security policies. Every query is scoped strictly to authenticated tenant session credentials, preventing cross-tenant data leakage.

Granular Role-Based Access Controls (RBAC): Administrative access is strictly limited to authorized personnel who require access to perform specific engineering or customer support duties, subject to mandatory multi-factor authentication and background checks.

Tax Document Cloaking: Social Security Numbers, ITINs, and FEINs stored in the Tax Vault are stored in dedicated encrypted partitions. UI display fields require active user interaction to unmask and trigger audit logs upon inspection.

While we implement cutting-edge security controls, no internet transmission or electronic storage system is 100% impenetrable. We cannot guarantee absolute security against all potential cyberattacks or unauthorized breaches.

---

12. CHILDREN'S ONLINE PRIVACY PROTECTION

The Service is strictly designed for commercial, professional, and adult personal financial management. The Service is not intended for or directed to individuals under the age of eighteen (18). We do not knowingly collect, solicit, or maintain Personal Information from children under the age of thirteen (13), nor do we have actual knowledge that we sell or share the Personal Information of consumers under sixteen (16) years of age.

If we learn that we have inadvertently collected Personal Information from a minor under 18 without verifiable parental consent, we will promptly delete that information from our active databases. If you believe a minor has provided information to us, please contact us immediately at contact@unifiedsolutionsgroup.co.

13. INTERNATIONAL DATA TRANSFERS & U.S. OPERATIONS

Unified Metrics is headquartered and operates within the United States. All data, servers, and processing facilities are located exclusively within the United States.

If you access the Service from outside the United States, please be aware that your information will be transferred to, stored, and processed in the United States, where privacy laws may not be as comprehensive as those of your jurisdiction of residence. By using the Service, you freely and explicitly consent to the transfer, storage, and processing of your Personal Information within the United States.

14. CHANGES TO THIS COMPREHENSIVE PRIVACY POLICY

We reserve the right to amend, update, or modify this Privacy Policy at any time to reflect changes in our legal obligations, data collection practices, or software features.

When we make updates, we will revise the Last Updated date at the top of this page.

If we make material changes that adversely affect your privacy rights or substantially expand our use of previously collected Personal Information, we will provide prominent advance notice through the Service (e.g., an in-app modal, banner alert, or direct email to your registered account address).

Your continued use of the Service following the effective date of an amended Privacy Policy constitutes your binding acknowledgment of and consent to the revised terms.

15. PRIVACY INQUIRIES & CONTACT INFORMATION

If you have questions, concerns, comments, or complaints regarding this Privacy Policy, our data practices, or our compliance with state and federal privacy laws, please contact our designated Privacy Officer at:

Unified Metrics

Attn: Legal Department & Privacy Officer

UNIFIED SOLUTION SERVICES CORP

664 S TAMIAMI TRAIL, SUITE C2

OSPREY, FL 34229

Email: contact@unifiedsolutionsgroup.co

Legal Inquiries: contact@unifiedsolutionsgroup.co

Support Website: https://unifiedsolutionsgroup.co/support

This document is provided for informational purposes and does not constitute legal, tax or accounting advice.