County IT Security & Compliance Packet

Architecture, Technical Controls, Subprocessors & HECVAT Lite-Aligned Self-Assessment | Effective November 23, 2026

Operator / Contracting Entity	Veduis LLC (Arizona Limited Liability Company, United States)
Service Scope	Remediate hosted PDF accessibility reading layer (widget & viewer) and signed-in customer client area (/app)
Security & Procurement Contact	Veduis LLC - Remediate Trust & Accessibility Team (https://remediatepdf.com/contact)
Support Hours	Monday-Friday, 08:00-17:00 Arizona time (MST); no 24/7 on-call staffing rotation
Vulnerability Disclosure Policy	https://remediatepdf.com/.well-known/security.txt
Status Page	https://remediatepdf.com/status

1. Plain-English SOC 2 & Audit Status

> **Our application runs on SOC 2 / ISO 27001-certified Cloudflare infrastructure. We provide our complete Security & Compliance Packet, HECVAT Lite self-assessment, VPAT 2.5Rev ACR, and Data Processing Addendum for customer review; formal independent CPA SOC 2 Type I attestation is planned on our compliance roadmap.**

- Independent CPA SOC 2 report: Not yet held. No self-certified SOC 2 claim is made.
- Third-party penetration test: Not yet contracted. Security hygiene is enforced through automated internal security test suites (tests/security-audit.js, tests/surface-boundaries.js, tests/provider-confidentiality-unit.js), GitHub dependency vulnerability alerts, and our published Vulnerability Disclosure Policy (/.well-known/security.txt).
- Commercial general / cyber liability insurance: Not currently carried; available prior to enterprise contract execution where required by municipal contract terms.

2. Zero-Customer-Infrastructure Architecture

Remediate requires no customer servers, virtual appliances, database maintenance, or CMS plug-ins. Customer websites install a single credential-free JavaScript snippet (/sdk.js) that discovers linked PDFs and renders an accessible in-page reading modal on the customer domain.

- Application & Edge Runtime: Cloudflare Pages Functions and Cloudflare Workers (remediate-ingest for scheduled site crawling and queued document preparation; remediate-ocr for on-platform OCR and large-PDF range processing).
- Data & Object Storage: Cloudflare D1 (SQLite database for tenant metadata, accounts, audit logs, and jobs) and Cloudflare R2 (private object storage for PDFs and generated transcripts, served solely through access-checked routes).
- On-Platform OCR & Selective Vision Fallback: Primary OCR for scanned, image-only PDFs runs automatically inside our Cloudflare-hosted container with no separate OCR vendor. On low-confidence, handwritten, or sideways scanned pages (capped at 10 pages per document), a transient rendered page image may be sent to our third-party AI processing provider for vision-assisted transcription and orientation detection unless AI processing is disabled for the workspace; transient page images are discarded immediately and never persisted.
- Strict Surface Isolation: Public marketing analytics (Google Analytics 4 and Microsoft Clarity) are never loaded inside the document viewer, the widget, the client area (/app/*), the admin panel (/admin/*), or authentication routes.

3. Technical Security Controls (Verified Against Current Build)

- Tenant Isolation & Least Privilege: Every document, scan, ticket, and usage event is scoped by tenant_id in D1. Private R2 objects are stored under opaque 32-character storage keys (docs/<key>/...) and served strictly through application routes that verify D1 tenant_id ownership and publication status before reading R2. Workspace roles are owner, admin, and member. Platform administration (/admin/*) is separate, requires MFA, and uses time-bounded, read-only, audited view-as grants for support diagnostics.
- Authentication & Session Security: Passwords are hashed with scrypt (N=16384, r=8, p=1, dkLen=64) using per-user 16-byte CSPRNG salts and constant-time comparison. Sessions use revocable secret-peppered SHA-256 token hashes (SHA-256(secret || token)) in HttpOnly; SameSite=Lax; Secure cookies (remediate_sid 7d, remediate_csrf 2d, remediate_mfa 10m). RFC 6238 TOTP 2FA includes 90-second single-use replay protection and hashed recovery codes.
- Transport & Browser Hardening: TLS enforced in production with HSTS (max-age=31536000; includeSubDomains), Content-Security-Policy (default-src "self", script-src "self" with public-site analytics allowlist, style-src "self" "unsafe-inline", form-action "self", base-uri "self"), X-Content-Type-Options: nosniff, X-Frame-Options: DENY (with verified-domain frame-ancestors on embed routes), Referrer-Policy: strict-origin-when-cross-origin, Permissions-Policy: camera=(), microphone=(), geolocation=(), Cache-Control: private, no-store on /app and /admin, and X-Robots-Tag: noindex on private/viewer surfaces.
- SSRF & Ingestion Protections: Every URL and redirect hop (up to 3 hops) is validated by cf/url-safety.js against the workspace verified domain allowlist; non-HTTP(S) schemes, embedded credentials, non-standard ports, IPv4/IPv6 literals, RFC 1918/link-local/CGNAT/loopback addresses, and cloud metadata endpoints are rejected.
- Audit Logging & Abuse Guards: Sign-ins, password/MFA changes, uploads, publishes, deletes, team changes, billing updates, and admin actions write to D1 audit_log. D1-backed rate limits and AI spend guards protect public endpoints from abuse.

4. Backups, Retention & Incident Response

- Database Backups: Daily automated export of D1 encrypted with age to an offline public key, SHA-256 checksum-verified, stored in a private GitHub repository (14-day daily, 90-day weekly/monthly retention), and verified via scripts/restore-drill.sh.
- Object Storage Disclosure: Document files in Cloudflare R2 are NOT currently mirrored to a second off-site location. Deleting a document removes both the database record and stored file immediately and cannot be recovered from backup.
- Breach Notification SLA (DPA Sec. 8): Initial notice within 24 hours and full written report within 72 hours of confirming a personal-data breach affecting customer data, with cooperation under A.R.S. Sec. 44-7501 and applicable customer state law.

Data Category	Retention & Deletion Policy
Customer documents & transcripts	Retained while active in the workspace until deleted by the customer or workspace closure. Deleting a document removes active R2 objects immediately.
Workspace deletion recovery archive	Restricted recovery archive retained up to 90 days after workspace closure before automated pruning (configurable between 30 and 90 days).
Encrypted D1 database backups	Exported daily via automated workflow, encrypted with age to an offline public key, SHA-256 checksummed, retained 14 days (daily) and 90 days (weekly/monthly).
Audit and security logs	Retained up to 12 months.
Reader accessibility requests & support tickets	Retained up to 24 months (tickets retained while account is active and up to 24 months after closure).
Aggregated usage analytics & lead records	Retained up to 24 months.
Email delivery metadata	Retained up to 180 days.
Translation & Q&A cache entries	Translation cache up to 12 months; Q&A cache up to 6 months; both purged when the parent document is deleted.
Rate-limit records	Retained up to 30 days after the limit window expires.
Billing and tax records	Retained for the statutory period required by law.

5. Published Subprocessors & AI Governance

The table below matches https://remediatepdf.com/legal/subprocessors. Any new or replacement subprocessor is posted at least 30 days before processing customer data, with a written right of objection under DPA Sec. 6.

Provider	Purpose	Data	Location
Cloudflare, Inc.	Hosting, Pages Functions, Workers, Queues, Containers (on-platform OCR), D1 database, and R2 object storage	Customer content, account data, logs, and backups	United States (with global edge delivery)
Resend, Inc.	Transactional email delivery and delivery status	Name, email address, message content, delivery metadata	United States
GitHub, Inc. (Microsoft Corporation)	Encrypted backup artifact storage in a private repository	Encrypted daily database export (account records, tickets, leads, audit log entries) and encrypted critical recovery assets (order forms, ticket attachments, deletion archives, and directly uploaded documents). Site-discovered document files are not included.	United States
Google LLC	Google Analytics 4 on public marketing pages only; optional translation provider when selected	Marketing analytics identifiers and page activity (never loaded in viewer or /app); document text submitted for translation if selected	United States and global
Microsoft Corporation	Microsoft Clarity heatmaps and session replay on public marketing pages only	Marketing analytics identifiers and interaction events (never loaded in viewer or /app)	United States and global
AI processing provider	AI document enrichment, selective vision-assisted OCR fallback on low-confidence/handwritten scans, translation, and cited question answering	Document text, transient rendered page images on selective low-confidence scanned pages (up to 10 pages/doc, never persisted), reader questions, and generated output	Worldwide
Stripe, Inc.	Invoice delivery and payment processing for customers on a paid agreement	Billing contact name and email, organization, invoice amounts, purchase order number, and payment status. Card and bank details are entered on Stripe's hosted invoice page only and are never received by Veduis.	United States and global

AI Processing Controls: AI processing is performed by a third-party AI processing provider rather than in-house. Automatic AI document enrichment and selective vision-assisted OCR fallback (transient page images on low-confidence/handwritten scans, capped at 10 pages/doc and discarded immediately) can be turned off for any workspace on request, leaving deterministic extraction and on-platform Cloudflare OCR only. Translation and cited Q&A run strictly when requested by a reader. We do not use customer documents to train models we operate. Because the AI processing provider operates globally (location: Worldwide) with no US-only data-residency guarantee, documents containing information restricted from leaving the United States should not be processed with AI features enabled.

6. HECVAT Lite-Aligned Vendor Self-Assessment

The self-assessment below mirrors core EDUCAUSE HECVAT Lite security, privacy, and procurement domains for county, municipal, and higher-education IT reviewers.

1. Company, Governance & Compliance Posture

ID	Control / Question	Veduis LLC Response
COMP-01	**Legal entity & operating jurisdiction**	Veduis LLC, an Arizona limited liability company operating from the United States. Governing law defaults to Arizona (Maricopa County), with written state/county venue elections available for Government Customers under Terms Sec. 15 and Sec. 17.
COMP-02	**Independent SOC 2 / ISO 27001 audit status**	No independent CPA SOC 2 report or ISO 27001 certificate is currently held. The application runs on Cloudflare's SOC 2 / ISO 27001-certified edge infrastructure; formal CPA SOC 2 Type I attestation is planned on our compliance roadmap.
COMP-03	**Third-party penetration testing**	No independent third-party penetration test report is currently available. Security controls are verified continuously through automated security regression suites (access control, tenant isolation, SSRF, surface-boundary, and provider-confidentiality checks), GitHub dependency vulnerability alerts, and an authorized public Vulnerability Disclosure Policy at /.well-known/security.txt.
COMP-04	**Commercial general / cyber liability insurance**	Not currently carried. Available prior to enterprise contract execution where required by a municipal procurement agreement.
COMP-05	**Published legal & trust commitments**	Terms of Service (/legal/terms, including Government Customer Sec. 17 clauses), Privacy Policy (/legal/privacy), Data Processing Addendum (/legal/dpa), Subprocessors (/legal/subprocessors), Accessibility Statement (/accessibility), VPAT 2.5Rev ACR (/accessibility/vpat), and dated change history (/legal/versions).

2. Architecture & Cloud Hosting

ID	Control / Question	Veduis LLC Response
ARCH-01	**Hosting model & customer infrastructure footprint**	Zero-customer-infrastructure hosted SaaS running on Cloudflare Pages Functions, dedicated Cloudflare Workers (scheduled site crawling, queued document preparation, and on-platform OCR / page-range processing), Cloudflare D1 (SQLite), Cloudflare R2 (private object storage), Cloudflare Queues, and Cloudflare Containers (on-platform OCR). Customers install only a single credential-free <script> tag on their website.
ARCH-02	**Multi-tenant logical isolation**	Every document, domain, scan, ticket, audit entry, and usage record is scoped by tenant_id in D1. Private R2 objects are stored under opaque 32-character storage keys (docs/<key>/...) and served strictly through application routes that verify D1 tenant_id ownership and publication status before reading R2. Platform admin routes (/admin/*) are strictly separated behind requireAdmin and mandatory MFA.
ARCH-03	**Analytics & tracking isolation**	Google Analytics 4 and Microsoft Clarity run exclusively on public marketing pages. They are never loaded in the document viewer (/docviewer.html, /v/*, /embed/*), the widget (/sdk.js), the client area (/app/*), the admin panel (/admin/*), or authentication screens.
ARCH-04	**Public widget security boundary**	The installable widget (/sdk.js) uses credential-free requests (credentials: "omit"), renders an in-page modal on the customer's domain (supporting strict frame-src "none" CSPs via local hydration), uses locally vendored pdf.js and pdf-lib with zero third-party script CDN dependencies, and sets X-Robots-Tag: noindex on viewer and document routes.

3. Identity, Authentication & Access Control

ID	Control / Question	Veduis LLC Response
AUTH-01	**Password hashing**	scrypt (N=16384, r=8, p=1, 64-byte derived key) with a per-user 16-byte cryptographically random salt and constant-time comparison (cf/passwords.js). Plaintext passwords are never logged or stored.

ID	Control / Question	Veduis LLC Response
AUTH-02	**Multi-factor authentication (MFA)**	RFC 6238 TOTP authenticator app support with constant-time verification, atomic monotonic time-step replay protection (users.totp_last_step), and SHA-256 hashed single-use recovery codes (cf/totp.js). Enabling or disabling MFA revokes sibling sessions and rotates the active session token. Optional for customer workspace users; mandatory for platform administrators.
AUTH-03	**Session & cookie hardening**	Opaque CSPRNG session tokens stored as secret-peppered SHA-256 hashes (SHA-256(secret || token)) in D1 with instant server-side revocation, per-device active session listing and one-click "Sign out all other devices" controls on /app/settings and /admin/security, and a 30-day absolute session lifetime ceiling (extendable in 7-day increments via keepalive). Cookies set HttpOnly, SameSite=Lax, and Secure in production (remediate_sid 7d, remediate_csrf 2d, remediate_mfa 10m), reinforced by Origin and Sec-Fetch-Site cross-site mutation guards.
AUTH-04	**Role-based access control (RBAC) & admin impersonation**	Workspace roles: owner, admin, member. Enterprise organizations support fleet-level owner/admin roles. Platform administrators may inspect a workspace only via time-bounded, audited, read-only view-as grants that reject write operations.
AUTH-05	**Enterprise SSO (SAML / OIDC)**	Not currently implemented. Workspace accounts authenticate via email/password + optional TOTP 2FA.

4. Data Protection, Encryption & AI Governance

ID	Control / Question	Veduis LLC Response
DATA-01	**Encryption in transit**	HTTPS/TLS enforced across all public, widget, API, and internal Worker endpoints with HSTS (Strict-Transport-Security: max-age=31536000; includeSubDomains).
DATA-02	**Encryption at rest**	Cloudflare D1 and R2 encrypt stored data at rest. Document originals and generated transcripts are stored as private R2 objects served solely through access-checked application routes; newly uploaded documents start in private draft status until explicitly published.
DATA-03	**Data residency & international processing**	Primary hosting operates in the United States on Cloudflare's global edge network. Some subprocessors - including the AI processing provider - operate globally (location: Worldwide) with no regional or US-only data-residency guarantee; customers requiring strictly US-confined processing may disable AI features on request or raise residency requirements before signing.
DATA-04	**AI data handling & opt-out controls**	AI document enrichment (and selective vision-assisted transcription on low-confidence, handwritten, or sideways scanned pages, capped at 10 pages per document with transient page images discarded immediately) runs via a third-party AI processing provider and can be disabled per workspace on request, leaving deterministic extraction and on-platform Cloudflare OCR only. Translation and cited Q&A run strictly when requested by a reader. Customer documents are never used to train models operated by Veduis. Any subprocessor change is posted 30 days ahead on /legal/subprocessors.
DATA-05	**Intended data classification**	Designed for publicly published government records (agendas, ordinances, budgets, public notices, reports) with a private pre-publish review workflow. Customers are responsible for redacting confidential, PII, CJIS, HIPAA, or FERPA-restricted data before publishing.
DATA-06	**Payment card (PCI) scope**	Zero cardholder data touches Veduis systems. All paid invoices and optional card/ACH payments are collected exclusively through Stripe's hosted invoice page or purchase-order invoicing.

5. Application Security, SSRF Protection & SDLC

ID	Control / Question	Veduis LLC Response
APP-01	**HTTP security headers**	Production responses enforce Content-Security-Policy (default-src "self", script-src "self" with public-site analytics allowlist, style-src "self" "unsafe-inline", form-action "self", base-uri "self"), X-Content-Type-Options: nosniff, X-Frame-Options: DENY (with verified-domain frame-ancestors only on embed routes), Referrer-Policy: strict-origin-when-cross-origin, Permissions-Policy: camera=(), microphone=(), geolocation=(), and Cache-Control: private, no-store on /app and /admin.
APP-02	**SSRF & document-fetching protections**	URL ingestion and website scanning validate every URL and up to 3 redirect hops through cf/url-safety.js: requires a verified workspace domain, allows only HTTP/HTTPS on standard ports (80/443), and blocks embedded credentials, IPv4/IPv6 literals, RFC 1918/link-local/CGNAT/loopback ranges, and cloud metadata hosts.
APP-03	**CSRF & abuse rate limiting**	State-changing browser routes enforce double-submit/session CSRF tokens. Login, password reset, accessibility requests, Q&A, translation, and scan starts enforce D1-backed rate limits and spend caps.
APP-04	**Audit logging**	Security-relevant events (sign-ins, password and MFA changes, document uploads/publishes/deletes, team changes, billing updates, view-as grants, and admin actions) write to D1 audit_log and are retained up to 12 months.
APP-05	**Vulnerability management & disclosure**	Automated GitHub dependency vulnerability alerts and pre-release test gates (security audit, surface boundaries, provider confidentiality, canonical URLs). Public security disclosure policy published at /.well-known/security.txt with a 2-business-day acknowledgment target.

6. Backups, Disaster Recovery & Incident Response

ID	Control / Question	Veduis LLC Response
BCDR-01	**Database backups & restore verification**	D1 database is exported daily via automated scheduled workflows, encrypted with age to an offline public key, SHA-256 checksummed, and retained 14 days (daily) / 90 days (weekly and monthly). Restore procedures are verified via periodic automated restore drills.
BCDR-02	**Object storage (R2) backup transparency**	Document files stored in R2 are NOT currently mirrored to a second off-site provider. Deleting a document removes both the database record and R2 object immediately and cannot be recovered from backup. Selected workspace records (order-form PDFs, support ticket attachments, deletion recovery archives, and directly uploaded files) may be included in encrypted backup archives under the same retention schedule.
BCDR-03	**Incident response & breach notification SLA**	Maintains a documented Incident Response Runbook reviewed every 6 months. DPA Sec. 8 commits to an initial breach notice within 24 hours and a full written report within 72 hours of confirming a personal-data breach affecting customer data, plus cooperation under A.R.S. Sec. 44-7501 and customer state law.
BCDR-04	**Service status & support staffing**	Live incident status is published at https://remediatepdf.com/status (database-backed, updatable without a code deploy). Support operates Monday-Friday, 08:00-17:00 Arizona time (MST) through our support team; there is no 24/7 on-call rotation.

7. Government Procurement & Accessibility

ID	Control / Question	Veduis LLC Response
GOV-01	**Public-sector contract protections**	Terms Sec. 17 explicitly supports Government Customers: order of precedence for required PO/procurement law, sovereign immunity preservation (A.R.S. Sec. 12-820 / state equivalents), non-appropriation termination without penalty, Net 45 / PO / arrears invoicing, tax-exemption certificates, no auto-charge renewals, and 60-day renewal reminders.

ID	Control / Question	Veduis LLC Response
GOV-02	**Public records / FOIA cooperation**	Terms Sec. 17.4 commits to notify the customer within 5 business days of any public-records request or subpoena for customer content and never independently waive customer exemptions.
GOV-03	**Product accessibility documentation**	Published VPAT 2.5Rev ACR covering WCAG 2.1 Level AA and Revised Section 508 at https://remediatepdf.com/accessibility/vpat (and downloadable tagged PDF).