DATA RETENTION POLICY

Information Security Program

Version 1.0

2026-05-22

Prepared for Walker-Miller Energy Services

Project Baseline, Inc. | Colorado | EIN 27-0639457 | todd@project-baseline.com | project-baseline.com

Entity: Project Baseline, Inc.

Effective date: 2026-05-22

Version: 1.0

Owner: Todd Walton, Information Security Officer / Data Protection Officer

Review cadence: Annual

1. PURPOSE

This policy defines what data Project Baseline, Inc. (PB) retains, for how long, in what location, and how it is disposed of when the retention period ends. The policy exists to (a) honor data minimization principles under CCPA and GDPR, (b) limit PB liability from unnecessary data accumulation, and (c) give clients and prospects a clear, written answer to "how long do you keep my data."

2. SCOPE

All PB-controlled data including:

- Client data (engagement deliverables, contracts, communications, uploaded documents)
- Prospect data (form submissions, AI Readiness inquiries, inquiry-form messages)
- Operational data (abuse-control logs, rate-limiting state, system logs)
- Generated content (AI-generated PDFs, reports, deliverables)
- Payment metadata (Stripe payment IDs, never card data, which PB does not store)

3. RETENTION SCHEDULE

DATA CATEGORY	STORAGE LOCATION	RETENTION PERIOD	DISPOSAL METHOD	JUSTIFICATION
Client engagement deliverables (consulting reports, contracts, working files)	Google Drive (PB Workspace), Todd's laptop, local working folders	Duration of engagement plus 7 years (statute of limitations for professional services claims in Colorado and Illinois)	Permanent delete from Drive and laptop; Trash purge confirmed	Legal and tax record retention
Client communications (email threads in todd@project-baseline.com Gmail)	Google Workspace	Duration of engagement plus 7 years; client may request earlier deletion of non-contractual messages	Permanent delete from Gmail, including Trash purge	Legal and tax record retention
Client uploaded documents (nonprofit-portal `./uploads/` directory)	DigitalOcean VPS local filesystem	90 days post-engagement OR 30 days post-account deletion, whichever is earlier	File-system delete plus secure overwrite via `shred -u` (Linux)	Privacy minimization; nonprofit-portal privacy policy commitment
Nonprofit-portal SQLite database records	VPS at `nonprofit-portal/db/database.sqlite`	Active accounts: retained for life of account; deleted accounts: 30 days then purged	SQL row delete plus SQLite VACUUM to reclaim space	Account lifecycle management
TAD AI Readiness abuse-control records (`_tad_abuse_guards.db`)	VPS at PB Report Engine path	90 days for rate-limiting and abuse-detection; aggregate metrics (no PII) may be retained indefinitely	Scheduled cron job purges rows older than 90 days, runs nightly	Abuse control requires recent history; older records have no operational value
TAD AI Readiness generated PDFs (`_generated_pdfs/`)	VPS at PB Report Engine path	7 days after email delivery to the requester	Cron job deletes files older than 7 days	PDFs are delivered via email and do not need long-term server storage

DATA CATEGORY	STORAGE LOCATION	RETENTION PERIOD	DISPOSAL METHOD	JUSTIFICATION
AI Readiness inquiry-form submissions (ai.project-baseline.com via FormSubmit.co)	todd@project-baseline.com Gmail inbox	2 years from receipt	Manual Gmail purge during annual data review (May each year)	Sales pipeline relevance window
Stripe payment metadata (PB-side: payment intent IDs, customer IDs, amounts; NOT card data)	nonprofit-portal SQLite, Stripe Dashboard	7 years per tax record requirements	Removed from local SQLite after 7 years; Stripe Dashboard retention is per Stripe's own policy	Tax record retention
Meeting recordings and transcripts (Fireflies.ai)	Fireflies cloud, occasionally exported to Drive	1 year in Fireflies; exports to Drive follow client engagement retention	Fireflies auto-purge per account settings; Drive purge per engagement schedule	Practical operational window
System logs (nginx access/error, application logs on VPS)	VPS local filesystem	30 days	Log rotation via logrotate, configured to 30-day retention	Operational troubleshooting window; longer storage creates unnecessary PII liability (IP addresses)
VPS abuse-control IP records	`_tad_abuse_guards.db`	90 days	Aligned with general abuse-control retention	Same rationale as above
Backups (database snapshots, document archives)	Encrypted off-VPS backup destination (see Backup Policy)	90 days rolling, plus annual snapshots retained for 7 years	Automated deletion per backup schedule	Recovery window plus annual archive for legal retention
Source code and infrastructure-as-code (GitHub repos, .env templates)	GitHub	Indefinite (operational requirement); secrets MUST NOT be committed	N/A	Operational requirement

DATA CATEGORY	STORAGE LOCATION	RETENTION PERIOD	DISPOSAL METHOD	JUSTIFICATION
Secrets (.env files containing API keys, tokens, credentials)	VPS local filesystem and Todd's laptop, NEVER GitHub	Active life of secret plus 30 days post-rotation	Rotate via provider; old secret value zeroed in .env and not retained	Security hygiene
Marketing list / newsletter subscribers (if PB launches one)	TBD email service (not currently active)	Active until unsubscribe; deleted within 30 days of unsubscribe per CAN-SPAM and GDPR	Provider-managed unsubscribe flow	Compliance requirement

4. SPECIAL RETENTION CASES

4.1 WALKER-MILLER TRADE ALLY SUBMISSIONS

Walker-Miller trade allies submitting via `walkermillertad.project-baseline.com/ai/` are treated as **prospect data, not client data**. Retention follows the TAD AI Readiness schedule above (90 days for abuse-control records, 7 days for generated PDFs, with the PDF also delivered by email to the requester who controls their own copy thereafter).

4.2 LEGAL HOLD

If PB receives notice of pending litigation, regulatory investigation, or subpoena affecting any data category, retention is **paused for all relevant data** until the legal matter is resolved. Todd documents the hold scope and start date in the Risk Register and resumes normal retention only after written closure of the matter.

4.3 CLIENT DELETION REQUESTS

Per the PB Privacy Policy, clients and prospects may request deletion of their personal data at any time. PB will:

1. Acknowledge the request within 7 days
2. Verify the requester's identity (email confirmation from the address of record, or government ID for high-sensitivity requests)
3. Complete deletion within 30 days of verified request
4. Confirm completion in writing

5. Retain only data PB is legally required to retain (for example, financial transaction records under tax law) and explicitly disclose what is retained and why

GDPR Article 17 (Right to Erasure) and CCPA Section 1798.105 (Right to Delete) requests are handled under this section.

5. DISPOSAL METHODS

STORAGE TYPE	DISPOSAL METHOD
Google Workspace (Gmail, Drive)	Delete + empty Trash (Google's deletion timeline applies thereafter, typically 30 days to full purge from Google systems)
SQLite databases	SQL DELETE plus VACUUM to reclaim space
VPS local files (PDFs, uploads, logs)	`shred -u` (overwrite plus delete) for sensitive files; `rm` for non-sensitive logs
Cloud SaaS (Stripe, Fireflies, etc.)	Use provider deletion API or dashboard delete; rely on provider deletion timeline (typically 30-90 days to full purge)
Endpoint files (Todd's laptop)	OS delete plus empty Trash; for sensitive files, use platform secure-delete tools (BitLocker-encrypted volumes provide cryptographic erasure on key destruction)
Backup files	Cryptographic erasure (delete encryption key) for encrypted backups; standard delete for unencrypted (note: per Backup Policy, all PB backups must be encrypted)

6. RETENTION AUDIT

Annual audit on or before May 22 each year reviews:

- Files in `_generated_pdfs/` older than 7 days (should be zero; if not, fix the cron purge)
- Rows in `_tad_abuse_guards.db` older than 90 days (should be zero; if not, fix purge)
- Files in nonprofit-portal `./uploads/` older than 90 days post-engagement (should be zero or actively engaged)
- Email retention in todd@project-baseline.com Gmail older than 7 years for client communications (purge as needed)

- Drive folder cleanup for engagements concluded more than 7 years ago

Audit log entry recorded in Security Awareness Training Record with date, items reviewed, and items purged.

7. OPEN ITEMS (MAY 22, 2026)

The following retention controls are stated in this policy but require implementation work in Section F before this policy is fully enforced:

1. Cron job on VPS to purge `_tad_abuse_guards.db` rows older than 90 days
2. Cron job on VPS to delete `_generated_pdfs/` files older than 7 days
3. Cron job or scheduled task in nonprofit-portal to purge deleted-account data after 30 days
4. Documented off-VPS backup retention schedule (90-day rolling + annual archive)
5. Documented annual retention audit process with calendar reminder

These items are tracked in the Security Controls Evidence document (Section F) and are Todd action items.

Signature: Todd Walton, Principal, Project Baseline, Inc.

Date: 2026-05-22

END OF DOCUMENT

Project Baseline, Inc. | Colorado | EIN 27-0639457 | todd@project-baseline.com | project-baseline.com