VENDOR AND SUB-PROCESSOR MANAGEMENT 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

Review cadence: Annual, plus event-driven on new vendor onboarding

1. PURPOSE

This policy defines how Project Baseline, Inc. (PB) selects, contracts with, monitors, and reviews third-party vendors and sub-processors that touch PB systems or data. It exists to (a) prevent supply-chain compromise of PB and PB-client data, (b) provide a registry of every external party with access to PB data, and (c) meet client and regulator requirements for vendor disclosure.

2. DEFINITIONS

"Vendor" means any third party providing services to PB. **"Sub-processor"** means a vendor that processes PB-controlled data on PB's behalf, including data PB processes for its clients. Sub-processors carry elevated requirements. **"Internal-only tool"** means a vendor that does NOT touch PB or PB-client data and is used only for internal operations (for example, an internal Telegram bot for system alerts).

3. ACTIVE VENDOR / SUB-PROCESSOR REGISTRY

The complete, current registry as of 2026-05-22 is below. All items derived from the PB Security Inventory (Section A) and verified through this Section B drafting.

3.1 SUB-PROCESSORS (CARRY PB OR PB-CLIENT DATA)

#	VENDOR	SERVICE	DATA FLOWING THROUGH	CONTRACTUAL BASIS	LAST REVIEWED
1	**Google LLC** (Google Workspace: Gmail, Drive, Docs, Sheets, Calendar)	Email, document storage, scheduling	All client communication, contracts, deliverables, meeting notes, attachments	Google Workspace Terms + Data Processing Amendment	2026-05-22
2	**Cloudflare, Inc.**	DNS, TLS, WAF, DDoS, CDN	Web traffic to all PB domains except walkermillertad (remediation pending Section F)	Cloudflare Self-Serve Subscription Agreement + DPA	2026-05-22
3	**GitHub, Inc. (Microsoft)**	Static site hosting (project-baseline.com, ai.project-baseline.com, www) + source code repos	Public marketing content; source code	GitHub Terms + DPA	2026-05-22
4	**Stripe, Inc.**	Payment processing for nonprofit-portal and (future) $99 audit reports	Payer email, name, payment instrument (Stripe-tokenized; PB never sees card data)	Stripe Services Agreement + DPA + PCI-DSS Level 1 attestation	2026-05-22
5	**FormSubmit.co**	Form relay for ai.project-baseline.com inquiry form	Name, email, business name, free-text message	Public terms of service only (free service, no DPA available). **Elevated risk: limited contractual protection.**	2026-05-22

#	VENDOR	SERVICE	DATA FLOWING THROUGH	CONTRACTUAL BASIS	LAST REVIEWED
6	**Anthropic, PBC**	AI generation for TAD AI Readiness Snapshot and PB Report Engine	Prospect-submitted business context (business name + trade + ZIP + brief pain points); no PII beyond email used for delivery	Anthropic Commercial Terms + Trust Center commitments (no training on API data)	2026-05-22
7	**OpenAI, L.L.C.**	Occasional AI use via API key in cos-webhook env (purpose pending Section F verification)	TBD	OpenAI API Terms	2026-05-22
8	**Google LLC (Gemini API)**	API key present in env (purpose pending Section F verification)	TBD	Google AI Studio Terms	2026-05-22
9	**Perplexity AI, Inc.**	Research lookups during consulting work	Search queries (no client PII)	Perplexity API Terms	2026-05-22
10	**Resend, Inc.**	Preferred email delivery for PB Report Engine (Gmail SMTP fallback)	Recipient email, subject, HTML body, PDF attachment	Resend Terms of Service + DPA	2026-05-22
11	**Fireflies.ai (Fred AI, Inc.)**	Meeting transcription (PB account plus TDC account)	Meeting audio plus transcripts of client and prospect conversations	Fireflies Terms + DPA	2026-05-22

#	VENDOR	SERVICE	DATA FLOWING THROUGH	CONTRACTUAL BASIS	LAST REVIEWED
12	**DigitalOcean, LLC**	VPS hosting (single droplet at 67.205.141.4)	All self-hosted application data, SQLite databases, generated PDFs, uploads	DigitalOcean Customer Agreement + DPA	2026-05-22
13	**Supabase, Inc.**	Database (TDC dashboard snapshots; PB usage pending Section F verification)	Pending Section F	Supabase Terms + DPA	2026-05-22
14	**The Rocket Science Group LLC d/b/a Mailchimp** (if used for any PB list)	Email marketing (not currently active for PB; placeholder)	N/A currently	Mailchimp Terms + DPA when active	N/A

3.2 INTERNAL-ONLY TOOLS (DO NOT CARRY PB OR PB-CLIENT DATA)

#	VENDOR	SERVICE	INTERNAL USE
1	Telegram (Telegram Messenger Inc.)	Bot API for internal alerts to Todd	COS briefs, security alerts, system status
2	Slack Technologies (Salesforce)	Internal alerts plus TDC integration	System notifications only for PB
3	Streak (Rewardly, Inc.)	CRM for TDC	Not actively used by PB
4	~~Monday.com~~	**PERMANENTLY DISABLED 2026-03-17.** Kill switch in MEMORY.md. Do NOT re-enable without explicit authorization.	N/A
5	ManyChat, Inc.	TBK and HHD social automations	No PB-client data
6	Buffer (Buffer, Inc.)	HHD social scheduling	No PB-client data
7	Automattic (WordPress for HHD)	HHD platform	No PB-client data
8	Plaid Inc.	Personal finance integration (Todd's personal accounts)	No PB-client data
9	Brave Software, Inc. (Brave Search API)	Research lookups	No PB-client data
10	Higgsfield, Canva, Stitch, Gamma, Figma, OneNote, Apify	Creative production tools	No PB-client data unless commissioned client work explicitly authorized

4. VENDOR VETTING REQUIREMENTS

Before onboarding a new vendor that will be a Sub-processor (touching PB or PB-client data), PB must complete:

1. **Risk classification.** High, medium, or low based on (a) data sensitivity, (b) volume of data, (c) vendor's own security posture, (d) regulatory exposure (CCPA, GDPR, sectoral).

2. **Security review.** - Request vendor's most recent SOC 2 Type II report, ISO 27001 certification, or equivalent third-party assessment - For high-risk vendors: complete a documented security questionnaire OR confirm the vendor publishes a Trust Center with sufficient detail - For medium-risk vendors: confirm vendor publishes a security overview and DPA - For low-risk vendors: confirm vendor has a privacy policy, an incident notification commitment, and TLS in transit
3. **Contractual review.** - Sub-processors must agree to a Data Processing Agreement (DPA) with breach notification SLA (PB requires no more than 72 hours) - For Sub-processors handling client data from PB clients with their own elevated requirements (HIPAA, GLBA, etc.), PB confirms the vendor agreement supports flow-down of those requirements before sub-processing client data - For free services without a DPA option (for example, FormSubmit.co): document the risk acceptance and limit the data sent to the minimum necessary
4. **Privacy policy disclosure.** Add new sub-processor to PB's published privacy policy at project-baseline.com/privacy within 30 days of onboarding.
5. **Registry update.** Add to Section 3 of this policy within 7 days of contract execution.

5. ONGOING MONITORING

Annual review of every Sub-processor on or before May 22 each year:

- Confirm vendor is still in business and the service is still in use
- Re-request current SOC 2 or equivalent (for vendors that provide one)
- Re-confirm DPA is current
- Review any publicized security incidents at the vendor in the prior 12 months
- Update risk classification if business model or data flow has changed
- Decide whether to renew, replace, or remove the vendor

Off-cycle review triggered by:

- Publicized breach at the vendor
- Vendor acquisition or material business change
- Material change in data flow (PB starts sending materially different data through the vendor)
- Regulatory change affecting vendor or data category

6. SUB-PROCESSOR DISCLOSURE TO CLIENTS

PB discloses the current Sub-processor list to clients via the public Privacy Policy at project-baseline.com/privacy. Clients receive at-least-30-days advance notice of material additions (new vendors handling their data) via the same channel and, for active engagements, by direct email.

Per CCPA and GDPR principles, clients may object to a new Sub-processor. Material objections trigger a conversation with the client about whether the engagement can continue under modified processing terms.

7. WALKER-MILLER SUB-PROCESSOR DISCLOSURE

For the WM subcontractor relationship specifically, PB will provide the current Sub-processor list as part of the Vanta assessment evidence package. Any future additions to the list during the WM engagement will be communicated to Nana Ellis (WM IT) at least 30 days in advance.

8. TERMINATION OF SUB-PROCESSOR

When PB terminates a Sub-processor relationship:

1. Confirm data return or destruction per the DPA (typical 30 days)
2. Rotate any credentials held by the Sub-processor
3. Remove integrations from PB systems
4. Update Sub-processor registry (Section 3) within 7 days
5. Update published Privacy Policy at next revision
6. Document termination in vendor file with date and reason

9. SPECIAL STATUS: FORMSUBMIT.CO

FormSubmit.co is the highest-risk active Sub-processor in PB's registry because it (a) operates as a free service with limited contractual protection, (b) relays form submissions through their infrastructure before reaching Gmail, and (c) has limited public security disclosure. The risk acceptance criteria:

- Volume: Low. The ai.project-baseline.com inquiry form generates a few submissions per month at most.

- Data sensitivity: Low to medium. Name, email, business name, free-text message. No payment data, no client data, no regulated data.
- Alternative: Migration to a same-origin form endpoint on PB infrastructure, or to a paid form service with a DPA (Formspree, Tally Pro, or similar). Target migration timeline: 90 days from policy effective date (by August 2026).

Until migration, FormSubmit.co is acceptable with the limitations documented here. Any prospect submitting via this form is, in effect, sending PB an email through a relay; PB does not represent the form as more secure than email.

10. OPEN ITEMS (MAY 22, 2026)

The following items in this policy require completion in Section F or shortly thereafter:

1. Verify whether OpenAI and Gemini API keys are actively used; remove from environment if dormant; update registry if active
2. Verify whether Supabase carries PB-client data; update registry accordingly
3. Confirm DPA execution status for every Sub-processor listed (most are accepted by SaaS Terms acceptance, but flag any missing)
4. Plan FormSubmit.co migration to same-origin or paid alternative within 90 days
5. Create internal vendor file folder at `output/project-baseline/_agency/vendors/` with one subfolder per Sub-processor containing DPA, terms of service, security overview, and renewal calendar

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