INFORMATION SECURITY 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.

Jurisdiction: Colorado Profit Corporation

EIN: 27-0639457

Effective date: 2026-05-22

Version: 1.0

Owner: Todd Walton, Principal and Information Security Officer

Review cadence: Annual, on or before May 22 each year

Framework alignment: NIST Cybersecurity Framework (CSF) 2.0

1. PURPOSE

This Information Security Policy establishes the security program for Project Baseline, Inc. (PB), a Colorado profit corporation operating as a solo consulting practice. The policy defines how PB protects the confidentiality, integrity, and availability of client data, prospect data, internal data, and PB intellectual property across all systems Todd Walton operates as the sole officer and principal.

This is the master policy. All other PB security policies (data retention, acceptable use, incident response, vendor management, access control, cryptography, backup, security awareness) operate under this document and inherit its definitions, roles, and scope.

2. SCOPE

This policy applies to:

- All systems owned, leased, or operated by PB, including the DigitalOcean VPS at 67.205.141.4 and all SaaS accounts enumerated in the PB Security Inventory (2026-05-22)
- All data PB collects, processes, stores, or transmits, including client data, prospect data, payment data (Stripe-tokenized), and AI-generated report content
- Todd Walton as the sole employee, officer, and operator
- Any future contractors, advisors, or sub-processors PB engages
- All AI agents operating under PB credentials (Anthropic, OpenAI, Gemini, Perplexity, Resend, FormSubmit.co, and others)

3. INFORMATION SECURITY ROLES

PB is a single-person firm. All security roles are held by Todd Walton.

ROLE	RESPONSIBILITY	HOLDER
Information Security Officer (ISO)	Overall security program ownership, annual policy review, incident response lead	Todd Walton
Data Protection Officer (DPO)	Privacy compliance (CCPA, GDPR where applicable), data subject request handling	Todd Walton
System Administrator	VPS administration, SaaS account management, MFA enforcement	Todd Walton
Incident Commander	First responder for any security incident, breach notification authority	Todd Walton

If PB engages contractors or employees in the future, this section will be updated within 30 days of the new role taking effect, and access control, NDA, and onboarding/offboarding procedures (see Access Control Policy and Confidentiality NDA Template) will be applied.

4. INFORMATION SECURITY PRINCIPLES

PB's security program is grounded in five principles aligned to NIST CSF 2.0 functions:

1. **Identify.** Maintain an accurate inventory of systems, data flows, and sub-processors. Annual review of the PB Security Inventory document.
2. **Protect.** Apply least-privilege access, MFA on every account that supports it, full-disk encryption on endpoints, TLS in transit, encryption at rest where the platform provides it, and rate limiting on public APIs.
3. **Detect.** Monitor for anomalous activity on the VPS (fail2ban, nginx access logs, application logs), abuse on public submission endpoints (flask-limiter, abuse-guards SQLite), and unauthorized changes to source code (GitHub commit notifications, branch protection on main).
4. **Respond.** Execute the Incident Response Plan with a 72-hour client notification SLA for confirmed breaches affecting client data.

5. **Recover.** Maintain off-VPS backups of databases and uploaded files, with documented restoration procedures (see Backup Policy).

5. RISK MANAGEMENT

PB performs an annual risk assessment covering:

- Public-facing web property exposure (5 domains/subdomains)
- VPS hosting (1 DigitalOcean droplet, 4+ services)
- Sub-processor dependencies (12+ active)
- Data retention liabilities
- Personnel access (single operator)

Risk register is maintained at `output/project-baseline/_agency/security/risk-register.md` (to be created within 30 days of policy effective date) and reviewed at minimum annually. High-severity risks identified outside the annual cycle (for example, from a Vanta-style external assessment) are added within 7 days of identification.

6. POLICY HIERARCHY

DOCUMENT	SCOPE
Information Security Policy (this document)	Master policy, roles, scope, principles
Data Retention Policy	What data PB keeps, for how long, why, and how it is purged
Acceptable Use Policy	How Todd (and any future PB personnel) use PB systems and data
Confidentiality / NDA Template	Required for any contractor or third party with access to PB or client data
Incident Response Plan	What PB does when something goes wrong, including 72-hour notification SLA
Vendor / Sub-processor Management Policy	How PB vets, contracts with, and reviews third-party services that touch PB or client data
Access Control Policy	Least privilege, MFA enforcement, role definitions, access review cadence
Cryptography Policy	TLS, password hashing, encryption at rest, key management
Backup Policy	What PB backs up, where, how often, and how restoration is tested
Security Awareness Training Record	Todd's annual self-attestation that he has reviewed all PB security policies and current threat landscape

7. ENFORCEMENT

All PB security policies are mandatory. Violations by Todd, contractors, or any party with access to PB systems will result in:

- Immediate access revocation for contractors or third parties
- Incident review and remediation per the Incident Response Plan
- For repeated violations by contractors: termination of engagement
- For breaches involving client data: notification to affected clients within 72 hours per the Incident Response Plan, and notification to any regulator with jurisdiction (CCPA, GDPR, sector-specific) per applicable law

8. POLICY REVIEW AND UPDATE

This policy is reviewed at minimum annually on or before May 22 each year. Triggers for off-cycle review include:

- New product launch (for example, the PB Report Engine $99 audit tier when it goes live)
- Onboarding of any contractor or employee
- Material change to sub-processor list (addition or removal of a service handling client data)
- Security incident requiring policy update
- Material change to applicable law (CCPA, GDPR, sectoral regulation)

Each review is logged in the Security Awareness Training Record with date, reviewer, and any changes made.

9. ACKNOWLEDGMENT

By operating PB systems, Todd Walton acknowledges he has read and understood this policy and all subordinate policies, and agrees to operate in accordance with them. Annual acknowledgment is recorded in the Security Awareness Training Record.

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