ACCEPTABLE USE 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

Applies to: All PB personnel (currently sole operator Todd Walton) and any future contractors, employees, or third parties with access to PB systems

1. PURPOSE

This Acceptable Use Policy (AUP) defines how PB personnel may use PB systems, data, and accounts. It exists to (a) prevent accidental misuse that creates security or legal exposure, (b) document expected behavior for any future contractors or staff, and (c) demonstrate to clients and auditors that PB has a written behavioral standard.

Because PB is currently a solo firm, this policy functions as Todd's self-attestation. It will scale to apply to any future personnel without modification.

2. SCOPE

Applies to use of:

- PB email accounts (todd@project-baseline.com primarily; other Google Workspace addresses for venture separation)
- PB VPS (DigitalOcean droplet at 67.205.141.4)
- PB SaaS accounts (GitHub, Stripe, Cloudflare, ManyChat, DigitalOcean, Anthropic, OpenAI, Resend, Fireflies, FormSubmit.co, etc.)
- PB local devices (Todd's Windows laptop, any future devices issued to staff or contractors)
- All client data, prospect data, payment data, and internal data PB controls

3. ACCEPTABLE USE

The following uses of PB systems are acceptable:

- Performing client consulting work for active PB engagements
- Operating and maintaining PB-owned tools (PB Report Engine, nonprofit-portal, marketing sites)
- Communicating with clients, prospects, vendors, and partners on PB business
- Internal PB operations (file management, accounting, reporting)
- Marketing and lead generation for PB services
- Personal communication on PB email is limited; primary personal email is a separate Google Workspace account already in use for venture separation

4. PROHIBITED USE

The following are prohibited on PB systems:

- Storing client data on personal cloud accounts (iCloud, personal Dropbox, personal Google Drive) outside PB-controlled Workspace
- Using PB credentials for non-PB purposes
- Committing secrets (API keys, passwords, tokens) to source control. Secrets live in `.env` files on VPS and laptop ONLY, never in GitHub
- Disabling MFA on any account where it is currently enabled
- Disabling full-disk encryption on any device used for PB work
- Disabling automatic security updates on the VPS or laptop without documented reason and timeline
- Using PB Anthropic or OpenAI API credentials to process data the client has not authorized for AI processing
- Sharing PB account passwords with anyone (including AI agents, which operate under API keys, not user passwords)
- Connecting unapproved third-party SaaS tools to PB Google Workspace (no OAuth grants to unknown apps without review)
- Downloading client data to unencrypted USB drives or removable media
- Discussing client confidential information in public channels (X, LinkedIn, podcast appearances) without explicit client consent

5. AI AGENT USE

PB operates an internal AI agent fleet (per the Kingdom OS / Chairman Todd agent system). These agents:

- Operate under PB-owned API credentials (Anthropic API key, OpenAI API key, etc.) stored in environment variables on Todd's laptop and the VPS
- Have no independent user identities or system access beyond what the calling shell session inherits
- Are subject to the same data handling rules as Todd. If a client has not authorized AI processing of their data, agents do not process it
- Are logged through standard system logging (terminal transcripts, cos-webhook logs, brain vault session memory). Sensitive client data flowing through agents is subject to the Data Retention Policy

6. PASSWORD AND MFA REQUIREMENTS

- Every PB SaaS account that supports MFA must have MFA enabled. Verified per Access Control Policy
- Passwords must be at minimum 14 characters, unique per account, stored in the PB-approved password manager (see Access Control Policy)
- No password reuse across PB accounts
- No password sharing
- Password manager itself must have MFA enabled and a strong master password

7. ENDPOINT REQUIREMENTS

Any device used for PB work must:

- Have full-disk encryption enabled (BitLocker on Windows, FileVault on macOS, LUKS on Linux)
- Auto-lock after 15 minutes of inactivity
- Require password or biometric to unlock
- Receive security updates within 14 days of release (auto-update preferred)
- Have endpoint antivirus or endpoint detection running (Windows Defender on Windows, built-in macOS XProtect on macOS, with current definitions)
- Be backed up to an encrypted backup destination per Backup Policy

8. REPORTING SECURITY EVENTS

Any PB personnel (including Todd as sole operator) who observes a potential security event must:

1. Trigger Incident Response Plan immediately
2. Document the event in the security-incident log
3. Escalate to the Information Security Officer (Todd Walton, in current single-operator state)
4. Preserve evidence (do not delete logs, files, or screenshots)
5. Notify affected clients per the 72-hour SLA in the Incident Response Plan if client data is involved

9. ENFORCEMENT

Violation of this policy is grounds for:

- For contractors: immediate termination of engagement
- For employees (none currently): disciplinary action up to and including termination
- For Todd: self-correction logged in the Risk Register; pattern of violations triggers a structural review of the policy

10. ACKNOWLEDGMENT

By operating PB systems, Todd Walton acknowledges he has read this Acceptable Use Policy and agrees to operate in accordance with it. Annual acknowledgment recorded in Security Awareness Training Record.

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

Date: 2026-05-22

END OF DOCUMENT