ACCESS CONTROL 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: Quarterly access review; annual policy review

1. PURPOSE

This Access Control Policy defines how Project Baseline, Inc. (PB) grants, reviews, and revokes access to PB systems and data. It exists to enforce least-privilege access, document the limited-personnel state of a solo firm, and prepare for orderly scaling when contractors or staff are added.

2. SCOPE

All PB systems including:

- VPS (DigitalOcean droplet at 67.205.141.4)
- SaaS accounts (Google Workspace, GitHub, Stripe, Cloudflare, ManyChat, DigitalOcean dashboard, Anthropic, OpenAI, Resend, Fireflies, and any others enumerated in Vendor Policy Section 3)
- Local endpoints (Todd's Windows laptop, any future PB-issued devices)
- Source code repositories
- Client data and prospect data

3. PRINCIPLE OF LEAST PRIVILEGE

All access is granted on a strictly-necessary basis:

- No standing access broader than the work requires
- No account sharing
- No "convenience" accounts that exceed role needs

- Time-limited elevated access where the tool supports it (for example, sudo on the VPS for specific tasks, not as a default shell mode)

4. ROLE DEFINITIONS (CURRENT AND FUTURE)

PB currently has one role: **Principal (Todd Walton).** All other roles below are forward-looking and apply when PB engages contractors or staff. Documenting them now allows orderly scaling.

ROLE	SCOPE OF ACCESS	EXAMPLES
Principal	Full administrative access to all PB systems	Todd Walton, sole operator
Contractor (Project)	Time-limited access to specific project files and tools	Future creative contractor for a specific deliverable
Contractor (Operations)	Time-limited access to specific operational systems	Future VA helping with calendar or inbox triage
Client User	Access to their own account in nonprofit-portal; no PB system access	Nonprofit portal end users
Auditor (Read-Only)	Time-limited read access for security or financial audits	WM IT auditor; financial accountant

5. ACCOUNT LIFECYCLE

5.1 PROVISIONING

For any new account or access grant:

1. Document the business need
2. Determine minimum access required (start with read-only or limited scope, expand only as necessary)
3. Provision via the platform's native access controls
4. Enable MFA before access is active
5. Set strong unique password stored in PB password manager
6. Add entry to Access Registry (Section 7)
7. Confirm scope with the receiving party (signed acknowledgment for non-PB personnel)

5.2 MODIFICATION

When role changes:

1. Re-assess minimum necessary access
2. Reduce scope first; expand only as new responsibilities require
3. Update Access Registry within 7 days

5.3 DEPROVISIONING

When access is no longer needed (contract end, role change, termination):

1. Revoke access within 24 hours (immediately for involuntary terminations)
2. Rotate any shared credentials the deprovisioned party may have seen
3. Recover PB-issued devices, if any
4. Update Access Registry
5. Confirm in writing the deprovisioning is complete

6. MFA REQUIREMENTS

Required on every account where the platform supports it. Non-negotiable.

Acceptable MFA factors (in order of preference):

1. Hardware security key (YubiKey, Titan)
2. TOTP app (Google Authenticator, Authy, 1Password TOTP, Bitwarden TOTP)
3. Platform-native authenticator (Apple Passkey, Google Smart Lock)
4. SMS as last resort and only where no other option is available (known to be weakest factor; flagged for upgrade)

Backup codes: Stored in PB password manager, never in plain text, never emailed.

MFA recovery: Documented per account in the password manager. Loss-of-device recovery plan exists for every account.

7. ACCESS REGISTRY

Maintained at `output/project-baseline/_agency/security/access-registry.md` (to be created within 30 days). Each entry includes:

FIELD	VALUE
Account / System	Name
Account holder	Todd or contractor name
Role	Per Section 4
Scope	What they can do
MFA enabled	Yes/No
MFA factor type	Per Section 6
Provisioned date	YYYY-MM-DD
Last reviewed	YYYY-MM-DD
Next scheduled review	YYYY-MM-DD
Termination date (if applicable)	YYYY-MM-DD

8. QUARTERLY ACCESS REVIEW

Every quarter on or before the 22nd of February, May, August, and November:

1. Walk through Access Registry
2. For each entry, confirm: still needed? Still correctly scoped? MFA still active?
3. Revoke anything no longer needed
4. Document review in Security Awareness Training Record
5. Flag anomalies in Risk Register

9. PRIVILEGED ACCESS

The following are considered privileged access and require additional scrutiny:

- VPS root or sudo access (currently: Todd only)
- DigitalOcean account ownership (currently: Todd only)
- Google Workspace admin (currently: Todd only)
- GitHub organization owner (currently: Todd only)

- Stripe administrator (currently: Todd only)
- Cloudflare account owner (currently: Todd only)
- Password manager master account (currently: Todd only)
- Domain registrar account (currently: Todd only)

Privileged access requirements:

- MFA with hardware key or TOTP (NOT SMS)
- Password rotation on any suspected compromise
- No sharing
- Quarterly review with explicit re-confirmation of need

10. SERVICE ACCOUNT AND API KEY MANAGEMENT

PB uses API keys for AI services (Anthropic, OpenAI, Gemini, Perplexity), Resend, Stripe, Cloudflare, and others.

API key requirements:

- Stored in environment variables on VPS and laptop ONLY
- Never committed to GitHub (enforced by Security Audit in Section F)
- Rotated at minimum annually OR immediately on any suspected compromise
- Scoped to least privilege where the provider supports it (for example, Stripe restricted keys for specific operations)
- Logged in a key inventory at `output/project-baseline/_agency/security/api-key-inventory.md` (to be created within 30 days) with provider, purpose, environment, creation date, last rotation, and next scheduled rotation

11. PHYSICAL ACCESS

PB has no separate office. Todd's home workspace at Broadview, IL is the physical access point for all PB systems.

Physical access controls:

- Locked home premises
- Devices auto-lock after 15 minutes

- BitLocker full-disk encryption on Todd's Windows laptop
- No PB-related papers (contracts, client data) left visible
- Visitors do not access PB workspace

For any future co-working or office space:

- Premises with controlled access (badged, locked)
- Devices remain locked when unattended
- Sensitive conversations conducted in private space (no client name and detail in open coffee shops)

12. REMOTE ACCESS

VPS access is exclusively via SSH with key-based authentication. Password authentication is disabled (to be verified in Section F). SSH keys stored in `~/.ssh/vps_key` on Todd's laptop with appropriate file permissions (0600).

Any future VPN or remote-management tooling will require MFA and will be added to this policy.

13. ACKNOWLEDGMENT

Todd Walton acknowledges he has read and agrees to operate in accordance with this Access Control Policy.

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

Date: 2026-05-22

END OF DOCUMENT