BACKUP 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 policy review; quarterly restoration test

1. PURPOSE

This Backup Policy defines what Project Baseline, Inc. (PB) backs up, how often, where, with what protections, and how restoration is tested. It exists to (a) protect against data loss from hardware failure, ransomware, accidental deletion, or vendor outage, (b) meet client expectations for business continuity, and (c) demonstrate to auditors that PB has a working recovery capability.

2. SCOPE

All PB data including:

- VPS SQLite databases (`_tad_abuse_guards.db`, `nonprofit-portal/db/database.sqlite`)
- VPS uploaded files (`nonprofit-portal/uploads/`)
- VPS configuration files (nginx config, systemd units, .env templates without secrets)
- VPS source code deployments (although source of truth is GitHub)
- Google Workspace data (Gmail, Drive, Docs, Sheets, Calendar)
- Todd's laptop working files
- Source code (mirrored from GitHub)
- Sub-processor data exports where PB needs an off-vendor copy (for example, Stripe transaction history export, Fireflies transcript export)

3. BACKUP SCHEDULE

DATA CATEGORY	BACKUP FREQUENCY	RETENTION	STORAGE DESTINATION	ENCRYPTION
VPS SQLite databases	Daily, automated via cron	90 days rolling + annual archive for 7 years	Off-VPS encrypted storage (Backblaze B2 free tier, AWS S3 free tier, or rclone to Google Drive)	AES-256 (PB-controlled key)
VPS uploaded files (`nonprofit-portal/uploads/`)	Daily, automated via cron	90 days rolling + annual archive for 7 years	Same as databases	AES-256 (PB-controlled key)
VPS configuration (nginx, systemd, .env templates)	Weekly, automated	90 days rolling	Same as databases	AES-256 (PB-controlled key)
DigitalOcean droplet snapshot	Weekly, optional ($2.40/month for snapshot storage)	4 snapshots rolling	DigitalOcean snapshot storage	Provider-managed
Google Workspace	Continuous (Google's native), plus quarterly export via Google Takeout to local encrypted archive	Quarterly archives retained 4 quarters; annual archives 7 years	Local encrypted external drive OR Backblaze B2	AES-256 on archive
Todd's laptop working files	Daily automated to cloud sync (OneDrive or Google Drive)	Continuous; version history per cloud provider	OneDrive or Google Drive (PB Workspace)	Provider-managed at rest; BitLocker on local device
Source code	Continuous push to GitHub	GitHub indefinite	GitHub primary; quarterly mirror clone to local encrypted archive	GitHub-managed; AES-256 on local archive
Sub-processor exports (Stripe, Fireflies, etc.)	Quarterly export to local encrypted archive	7 years	Local encrypted external drive	AES-256 on archive

4. BACKUP DESTINATION CHOICE

Primary recommendation: Backblaze B2.

Rationale:

- $0/month for the first 10 GB of storage and 1 GB/day of egress (PB's volume fits comfortably within free tier today)
- Native client-side encryption support via rclone
- S3-compatible API for automation
- US-based with documented security posture

Alternative: rclone to a dedicated Google Drive folder in PB Workspace.

Rationale:

- Already paying for Google Workspace
- No additional vendor onboarding
- rclone provides client-side encryption (`crypt` remote)
- Acceptable if Backblaze B2 onboarding is delayed

Local archive (secondary, not primary): Encrypted external drive at Todd's workspace.

Rationale:

- Air-gapped from internet during backup-not-running periods
- Useful for ransomware resilience
- NOT a replacement for cloud backup (single point of failure)

5. ENCRYPTION STANDARD FOR BACKUPS

All cloud-stored backups encrypted with AES-256 using a PB-controlled encryption key. The encryption key:

- Generated using platform CSPRNG
- Stored in PB password manager
- Backed up secondarily (sealed envelope in safe; secondary password manager) so Todd can decrypt even if primary password manager is unavailable
- Rotated annually with re-encryption of the most recent backup set under the new key

- Old key retained in PB password manager for 90 days post-rotation to support restoration from older backups

6. RESTORATION TESTING

Quarterly restoration test on or before the 22nd of February, May, August, and November:

- Pick one data category at random
- Restore the most recent backup to a test environment (a temporary droplet, a sandbox folder, etc.)
- Verify the restored data is complete and usable
- Document the test in `output/project-baseline/_agency/security/backup-restoration-log.md`
- If the test fails, immediately remediate the backup process and re-test within 7 days

7. BACKUP MONITORING

Daily automated backup jobs MUST report success or failure:

- Successful backup: log entry written, Telegram notification suppressed (success is the default expectation)
- Failed backup: Telegram alert to Todd from cos-webhook, with the failing job name and timestamp
- Two consecutive failures: Sev-2 incident, triggers Incident Response Plan investigation

Weekly health-check confirms most recent backup timestamps for every category are within expected windows.

8. RECOVERY TIME AND RECOVERY POINT OBJECTIVES

For a solo consulting firm, formal RTO and RPO targets are scoped to the actual business impact:

DATA CATEGORY	RPO (MAX DATA LOSS)	RTO (MAX DOWNTIME)
nonprofit-portal SQLite	24 hours	24 hours
nonprofit-portal uploads	24 hours	48 hours
TAD AI Readiness data	24 hours	72 hours (low business impact; prospects can resubmit)
Google Workspace	Continuous (provider RPO)	Provider-dependent
Source code	Continuous (GitHub)	1 hour (clone fresh)
VPS configuration	7 days	4 hours (reconstructible from documented setup process)

If actual restoration test reveals these targets cannot be met, update the targets to match reality and remediate the backup process to close the gap.

9. DISASTER SCENARIOS

SCENARIO	RECOVERY APPROACH
VPS ransomware	Provision fresh VPS, restore from latest backup, rotate ALL credentials, audit for re-infection vector
VPS hardware failure	Provision fresh VPS, restore from latest backup or DigitalOcean snapshot, redeploy code from GitHub
Accidental deletion in nonprofit-portal	Restore affected rows or files from most recent daily backup; document via Incident Response Plan
Google Workspace account compromise	Engage Google security via Workspace admin; restore from quarterly Takeout export if needed
GitHub account compromise	Engage GitHub support; restore from local mirror clone; rotate all repository deploy keys and webhook secrets
Backup destination compromise	Migrate to alternate destination; new encryption key; verify restoration in new destination

10. OPEN ITEMS (MAY 22, 2026)

The following are not yet implemented and are tracked in Section F:

1. Set up Backblaze B2 account (free tier) OR configure rclone-encrypted Google Drive folder
2. Write cron job on VPS to back up SQLite databases nightly to selected destination
3. Write cron job on VPS to back up nonprofit-portal/uploads/ nightly
4. Write cron job on VPS to back up nginx and systemd config weekly
5. Schedule first quarterly Google Workspace Takeout export
6. Configure backup monitoring alerts via cos-webhook to Telegram
7. Run first restoration test within 30 days of policy effective date
8. Document encryption key recovery procedure (secondary copy location and format)

These items are Todd action items and require approximately 4 hours of setup work plus 1 hour quarterly thereafter.

11. ACKNOWLEDGMENT

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

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