TactiFunds Privacy Policy

Last updated: June 9, 2026 **Effective date:** June 9, 2026

This Privacy Policy describes how **Tristar Dynamics LLC** ("we," "us," "our") collects, uses, stores, and shares information when you use the **TactiFunds** mobile application (the "App"). By using the App, you agree to the practices described here. If you do not agree, do not use the App.

TactiFunds is an independent product. **It is not affiliated with, endorsed by, or sponsored by the U.S. Department of Defense, any branch of the U.S. Armed Forces, or any federal government agency.** Pay tables, allowances, and benefit figures reference publicly available DoD and VA data and are provided for informational purposes only. The App does not provide financial, tax, legal, or investment advice.

---

1. Who we are

Controller: Tristar Dynamics LLC **Product:** TactiFunds (iOS application) **Contact:** tactifunds@gmail.com

If you have questions about this policy, your data, or want to exercise any of the rights described below, contact us at the email above.

---

2. What information we collect

We try to collect as little as possible. Here's everything the App handles, grouped by source.

2.1 Information you provide

When you create an account or use the App, you provide:

- **Account information:**
- Email address (for email/password sign-in), **OR**
- Apple ID identifier and name (if you choose Sign in with Apple). Apple only shares your name with us once, the first time you sign in.
- A display name you can edit.
- **Financial planning inputs you enter into the App's tools:**
- Pay grade, branch of service, years of service, dependents, ZIP code (for BAH lookup)
- TSP balance, contribution percentages, fund allocations, retirement target year
- Tax filing status and dependent count
- Savings goals, debts, debt-payoff strategy
- Spouse income, retirement, and budget data (if you choose to enter it)
- VA disability ratings, deployment plans, SGLI coverage choices, SDP deposits

- Budget items, daily expenses, monthly snapshots
- Inputs to planning tools (PCS, Separation, VA Home Loan, GI Bill, Pension, etc.)
- Mission and badge progress within the App
- **LES (Leave & Earnings Statement) uploads:** When you upload an LES PDF, the App parses it on your device to extract structured fields (gross pay, deductions, allotments, leave balance, etc.). **The raw text of your LES is never stored or transmitted.** Only the parsed numeric fields and your pay date are saved.
- **Feedback you submit** through the in-app Feedback Board (post titles, descriptions, comments, upvotes). Posts are public to other TactiFunds users.
- **Profile photo** (optional). If you set one, it's stored locally and synced to your account.

2.2 Information we collect automatically

- **Subscription status** from Apple's StoreKit framework: which subscription tier you have, whether you're in a trial, and transaction identifiers needed to verify your entitlement. **We never see your credit card, debit card, or bank information.** All payment processing is handled by Apple under Apple's privacy policy.
- **Anonymous device identifier** for the Feedback Board's voting system: a randomly generated UUID is stored on your device so the App can prevent duplicate upvotes on the same post. This identifier is not linked to your account or any personal information.
- **Diagnostic logs** from Apple's standard frameworks may surface in your device's system logs (e.g., crash reports you choose to share with Apple). We do not operate our own analytics SDK and do not collect usage telemetry, page views, click streams, or session recordings.

2.3 Information we do not collect

We deliberately don't collect or ask for:

- Social Security Number, passport number, or other government identifiers
- Bank account numbers, routing numbers, or wire details
- Credit card or debit card numbers (Apple handles all payments)
- Your contacts, photos library (other than a profile photo you select), microphone, camera, or location
- Browsing history, web tracking data, or cross-app tracking identifiers (the App does not request App Tracking Transparency permission and does not track you across apps or websites)
- Health or biometric data

---

3. How we use your information

We use the information you provide to:

- **Operate the App's features.** Your financial inputs power the calculators, planners, missions, and personalized recommendations you see in the App.

- **Save your progress** so your data is there when you reopen the App.
- **Sync your data across your iOS devices** if you sign in with the same account.
- **Verify your subscription tier** and unlock the features you've subscribed to.
- **Deliver in-app notifications** you've opted into (e.g., payday reminders, separation milestones, badge earns).
- **Respond to feedback you submit** through the Feedback Board.
- **Communicate with you about service issues** (e.g., security incidents, material changes to this policy).

We do **not** use your information for advertising. We do not sell, rent, or trade your information. We do not use your data to train machine-learning models — yours or anyone else's.

---

4. How we store and protect your information

4.1 Encryption at rest

All financial data the App persists on your device is **encrypted with AES-GCM** before being written to local storage. The encryption key is generated on your device, stored in the iOS Keychain with `kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly`, and **never leaves your device** — not even to iCloud Keychain backup.

4.2 Cloud storage

When you sign in, your encrypted state is also stored in our cloud database (operated by Supabase, see Section 5) so you can access it from your other iOS devices. The cloud database enforces **row-level security**: each row is locked to the user who owns it, and our application code performs an additional ownership check before applying any cloud data.

4.3 Authentication

- **Email/password authentication** uses industry-standard password hashing handled by our authentication provider. We never see your password in plaintext.
- **Sign in with Apple** uses Apple's privacy-preserving identity flow. Apple may provide us with a per-app private email relay address; emails sent to it are forwarded to your real email by Apple.

4.4 In transit

All network traffic between the App and our servers uses HTTPS/TLS encryption.

4.5 Retention

- **Account and financial data:** Retained as long as your account is active. You can delete it at any time using the controls in Section 7.
- **Feedback posts and comments:** Retained indefinitely so other users continue to see the discussion. You can request removal of your specific contributions by emailing us.

- **LES uploads:** Only the parsed fields are retained, on the same schedule as your account. Raw LES text is never persisted.

---

5. Who we share information with

We only share information with the limited third parties needed to operate the App:

Provider	Purpose	What they receive
Apple Inc.	App distribution, Sign in with Apple, in-app purchases, push of local notifications	Your Apple ID identifier (only for Sign in with Apple), purchase receipts. Subject to Apple's Privacy Policy.
Supabase, Inc.	Authentication, encrypted database hosting	Your account email or Apple ID, your encrypted financial state blob, feedback posts/comments. Subject to Supabase's Privacy Policy.

We do not share data with advertising networks, data brokers, or analytics vendors.

We may disclose information **if legally required** by valid court order, subpoena, or other legal process — but only to the extent legally compelled, and we will notify you when permitted to do so by law.

In the unlikely event of a corporate transaction (merger, acquisition, sale of assets), user information may be transferred to the successor entity. You will be notified of any such change via the App or your registered email.

---

6. International data transfers

The App is offered in the United States. Our cloud infrastructure may be located in the United States. If you access the App from outside the United States, your information will be transferred to and processed in the United States, where data protection laws may differ from those in your jurisdiction. By using the App, you consent to this transfer.

---

7. Your rights and choices

You can manage your data directly in the App at any time:

- **View and edit your data:** Every value the App stores is visible in the corresponding tool — there is no hidden profile.
- **Export:** Contact us at the email above and we will provide a copy of your data in a machine-readable format within 30 days.

- **Delete all your data (keep your account):** Settings → Danger Zone → **Delete All My Data**. This permanently removes every value you've entered, on this device and from our cloud. Your account stays active. We rotate the device encryption key during this process so any residual encrypted data on backups cannot be recovered.
- **Delete your account entirely:** Settings → Danger Zone → **Delete My Account**. This deletes your authentication record, all financial data, and your profile photo from our systems. You will be signed out immediately. You cannot reactivate a deleted account, but you can create a new one.
- **Notification controls:** Settings → Preferences → **Notifications**, or in iOS Settings → TactiFunds.

Region-specific rights

Depending on where you live, you may have additional rights under applicable law:

- **California residents (CCPA/CPRA):** the right to know what personal information we hold about you, the right to delete it, the right to correct inaccuracies, the right to opt out of sale or sharing (we do not sell or share personal information for cross-context behavioral advertising), and the right not to be discriminated against for exercising these rights.
- **EU/EEA residents (GDPR):** the right to access, rectification, erasure, restriction, data portability, and to object to processing. Our legal basis for processing is your consent (when you create an account and enter data) and contract performance (operating the App you've subscribed to). You may also lodge a complaint with your local data protection authority.
- **UK residents (UK GDPR):** the same rights as EU residents, with the ICO as the supervisory authority.
- **Other jurisdictions:** contact us and we will work with you to honor any applicable local rights.

To exercise any of these rights, email us at the address in Section 1. We will respond within 30 days (or the timeframe required by your jurisdiction's law, if shorter).

---

8. Children's privacy

The App is intended for users **aged 17 or older**. We do not knowingly collect personal information from children under 13. If you believe a child under 13 has provided us with personal information, contact us and we will delete it promptly.

The App is rated 17+ in the App Store because of its references to financial decisions, military service-related content, and adult subject matter (e.g., disability ratings, life insurance).

---

9. Security caveats

We take security seriously, but no system is perfectly secure. You can help protect your account by:

- Using a strong, unique password (or Sign in with Apple, which generates a unique credential per app)
- Keeping your iOS device updated and protected with a passcode/Face ID/Touch ID
- Signing out on shared devices

If we become aware of a security incident affecting your data, we will notify you in accordance with applicable law.

---

10. Changes to this policy

We may update this Privacy Policy from time to time — for example, when we add new features or change our service providers. When we do, we will:

- Update the "Last updated" date at the top.
- For material changes, notify you in the App and/or by email before the new policy takes effect.

Continued use of the App after changes take effect means you accept the updated policy. If you don't agree, you can delete your account at any time.

---

11. Contact

Questions, complaints, or requests:

Tristar Dynamics LLC · 2 Arnot St, Ste 6 #1053, Lodi, NJ 07644 · tactifunds@gmail.com

For legal process and law-enforcement requests, please use the email above with subject line "Legal Request."
