WishLane — AML / CTF & Sanctions Policy

Platform: WishLane (wishlane.com) **Business model:** Donation-based personal crowdfunding platform **Payments:** Stripe Connect (Express) + Stripe Checkout **Document type:** Anti-Money-Laundering / Counter-Terrorist-Financing / Sanctions policy **Last updated:** July 4, 2026 **Owner / compliance contact:** John Akyiano — jakyiano@gmail.com

1. Purpose & scope

This policy sets out how WishLane manages money-laundering (ML), terrorist-financing (TF), and sanctions risk across its donation-based crowdfunding platform. It applies to all campaigns ("wishes"), organizers ("creators"), recipients, and contributions ("donations, fulfilments, and gift purchases") on wishlane.com. It consolidates the controls that answer this compliance dashboard, including **how WishLane verifies the legitimacy of campaigns, organizers, and intended recipients**, **how campaigns are made transparent to donors**, and **how each campaign is assigned a risk rating**.

WishLane is a technology platform, **not** a bank, money transmitter, money services business, or other regulated financial institution, and is not itself licensed or registered by any financial regulator (see Terms of Service §5). All payment processing, settlement, recipient identity verification, and sanctions screening of connected accounts are performed by our payment provider, **Stripe**. This policy describes both the functions WishLane relies on Stripe for and the additional controls WishLane operates itself.

2. Governance & roles

- A designated **compliance contact** (John Akyiano, jakyiano@gmail.com) owns this policy, monitors alerts, reviews campaigns, handles escalations and takedowns, and maintains records.
- WishLane takes a **risk-based approach**: controls are proportionate to the platform's assessed ML/TF/sanctions risk, which is documented in the **Sanctions Risk Assessment** and reviewed at least annually under the **Independent Review Policy**.

3. Verifying campaigns, organizers, and recipients

WishLane verifies legitimacy at three points: the **account/organizer**, the **recipient (payout) identity**, and the **campaign itself**.

3.1 Organizer / account verification

- Creating a campaign requires a registered WishLane account with a **verified email address** (email verification is mandatory; a one-time-passcode option is also supported). Login is rate-limited with account lockout to deter automated abuse and account takeover.
- The organizer of a campaign is the account holder who publishes it and is the party who must complete recipient (payout) verification below before any funds are released.

3.2 Recipient (payout) identity verification — KYC

- No campaign can receive disbursed funds until the recipient completes **Stripe Connect Express** onboarding. Stripe performs full identity/KYC verification of the recipient — representative identity, government ID, and bank account — and screens the connected account against sanctions lists.
- **Money never reaches a recipient until Stripe has verified their identity.** Contributions to a not-yet-verified recipient are **held in the WishLane platform balance** and released via Stripe transfer only after verification completes.

3.3 Campaign legitimacy verification

Every campaign is checked at creation and on edit:

- **Automated risk rating** (see §4) scores the campaign from its content and category and drives automated gating of higher-risk campaigns.
- **Prohibited-use screening.** Campaigns are subject to a published **Acceptable Use Policy** that enumerates prohibited categories aligned with Stripe's Restricted Businesses list; anything prohibited by Stripe is prohibited on WishLane.
- **Administrative moderation.** An administrator is notified of every new campaign and can, at any time, **suspend, archive, delete, or require Stripe verification before donations** on any campaign through an administrative portal.
- **Automated containment.** High-severity transaction-monitoring alerts automatically suspend a campaign pending review (see §6).

4. Campaign risk rating

Every campaign is assigned a **risk rating of low, medium, or high** at creation and re-evaluated on edit. The rating is **deterministic and explainable** — each campaign records the specific signals ("flags") that drove its rating, so a reviewer can see *why* it was rated as it was.

Inputs to the rating:

Factor	Effect
Prohibited / high-risk keywords in the title or description (e.g. investment, lending, crypto, weapons, gambling, adult, controlled substances, bail/ransom — aligned with the Acceptable Use Policy)	Any match → **high**
Goal amount above the high threshold (default $50,000)	Strong upward weight
Goal amount above the elevated threshold (default $10,000)	Moderate upward weight
Elevated category (business, charity, other)	Moderate upward weight

Outcome:

- **High** — any prohibited/high-risk keyword match, or a combination of goal and category factors reaching the high threshold. **High-risk campaigns are automatically gated: donations are blocked until the creator completes Stripe verification**, so funds cannot be held for an unverified recipient on a high-risk campaign.
- **Medium** — an elevated combination of goal and category factors.
- **Low** — ordinary personal-need campaigns.

Thresholds are centrally configurable. The rating is stored on the campaign, surfaced to administrators (with filtering by risk level), and feeds moderation decisions.

5. Transparency to donors

Contributions are transparent and tied to a specific, visible campaign:

- Each campaign publicly displays its **title, description, category, goal amount, funds raised to date, images**, and the organizer.
- Every contribution is **tied to a specific campaign**; donors choose a campaign and, optionally, a specific registry item to fund.
- **Platform fees are disclosed to donors at checkout**, and payment is processed by Stripe on a hosted, secure checkout page.
- Donors may choose to contribute **anonymously to other users**, but the contribution remains recorded and tied to the campaign for monitoring and reconciliation.
- All governing **policies are public** — Terms of Service, Acceptable Use Policy, Refund Policy, Privacy Policy — and the platform's fraud/monitoring controls are summarized publicly at wishlane.com/security.

6. Transaction monitoring

WishLane operates a layered transaction-monitoring program on every contribution:

- A **deterministic, rule-based engine** screens for ML/fraud signals — campaign and donor velocity, structuring (repeated amounts just under a review threshold), and donor concentration — and raises an alert when any signal trips.
- An **AI-assisted analysis layer** (built on Anthropic's Claude, decision-support only, aggregated data) reviews each flagged case and produces an independent risk read and recommended action for a human reviewer.
- **High-severity alerts auto-suspend** the campaign pending review; all alerts are worked through an administrative queue where a reviewer clears, escalates, or reopens them, with reviewer identity and timestamp recorded.

The monitoring program is documented in full in the **Transaction Monitoring Program** document and summarized at wishlane.com/security.

7. Sanctions & counter-terrorist-financing controls

- **Sanctions screening.** WishLane relies on **Stripe** to screen connected (recipient) accounts against applicable sanctions lists, and on Stripe and the card networks for controls on card payments. WishLane does not presently perform independent sanctions-list screening; the scope of donor-side screening is an open item being confirmed with Stripe and is tracked in the Sanctions Risk Assessment.
- **Prohibited purposes.** The Acceptable Use Policy prohibits any campaign that funds or promotes terrorism, violence, or hate, and any activity prohibited by Stripe or by law.
- **Geographic footprint.** WishLane serves a US/Canada, USD footprint; recipients are limited to Stripe-supported countries, and sanctioned-jurisdiction exposure is mitigated by Stripe's connected-account and payment controls.
- **Risk assessment.** Sanctions/TF exposure is documented and rated in the **Sanctions Risk Assessment**, reviewed at least annually.

8. Contribution limits & held funds

- **Limits enforced before payment:** minimum $1 and maximum $10,000 per single contribution; maximum $10,000 per registered donor per campaign; maximum $100,000 raised per campaign. Over-limit attempts are rejected before payment. (Values are centrally configurable.)
- **Manual review:** any single contribution over a set threshold (default $200) is held for manual review before release.
- **Held funds:** contributions for unverified recipients are held in the platform balance and released only after Stripe verification.

9. Dispute, refund & fraud handling

Signed, idempotent Stripe webhooks automatically reverse refunded or disputed amounts — removing them from the campaign total and clawing them back from any still-held funds. Stripe Radar runs on all card charges. The Refund Policy asks contributors to contact WishLane before filing a dispute; refunds are issued where funds have not been disbursed or where fraud is found.

10. Recordkeeping

WishLane records all donations, fulfilments, gift purchases, and payouts; every monitoring alert (signals, severity, amount, AI assessment); every alert resolution with reviewer identity and timestamp; and refund/dispute reconciliations. Records support audit, independent review, and production to payment partners or regulators on request.

11. Training

All relevant personnel receive AML/CTF and sanctions training at onboarding and at least an annual refresher, per the **AML/CTF & Sanctions Training Policy**. WishLane is currently founder-operated; the policy applies to any personnel engaged.

12. Independent review

This policy and the wider program are subject to **independent review at least annually** and upon material change, per the **Independent Review Policy**. Completed reviews are recorded in the Compliance Review Log.

13. Reporting & escalation

Suspected violations, suspicious activity, or sanctions concerns are escalated to the compliance contact, who may **freeze or reverse contributions, suspend or remove campaigns and accounts, refund contributors, and report unlawful activity to Stripe and to the appropriate authorities.**

14. Related documents

Document	Covers
Transaction Monitoring Program	The rule-based + AI-assisted monitoring program (public: wishlane.com/security)
Sanctions Risk Assessment	Rated ML/TF/sanctions exposure and action items
Independent Review Policy	Annual independent review commitment (public PDF)
AML/CTF & Sanctions Training Policy	Onboarding + annual refresher training
Crowdfunding Risk Controls	Overall platform risk controls for Stripe review
Acceptable Use Policy	Prohibited campaigns (public: wishlane.com/acceptable-use)

Policy governance

This policy is owned by the compliance contact, reviewed at least annually and upon any material change to the payment flow, risk profile, or applicable law, and made available to payment partners and regulators on request. Thresholds and figures are centrally configurable and current as of the date above.