BUROHELP ANTI-FRAUD & ANTI-MONEY-LAUNDERING (AML) POLICY

This Policy outlines how the Foundation prevents, detects, and responds to fraud, corruption, money laundering, terrorist financing, and other integrity risks. It ensures compliance with Dutch law, including the **Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT)**, ANBI rules, and general nonprofit governance standards.

1. Definitions

- **"Foundation"** — Stichting Burohelp.
- **"Fraud"** — intentional deception for unlawful or private gain, including misappropriation of funds, falsification of records, and manipulation of Time Bank data.
- **"Money Laundering"** — disguising the origin of criminal proceeds to appear legitimate.
- **"Terrorist Financing"** — providing assets for terrorist activities.
- **"WWFT"** — the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act.
- **"Donor"** — any entity providing financial contributions.
- **"Nonprofit"** — ANBIs/PBOs/NGOs supported by the Foundation.
- **"User"** — any person using the Burohelp Platform.
- **"Suspicious Activity"** — any transaction or behaviour that appears inconsistent with lawful or public-benefit objectives.
- **"Due Diligence"** — checks performed on donors or Nonprofits prior to accepting or allocating funds.

2. Purpose of This Policy

The Foundation adopts this Policy to:

1. Prevent misuse of the Platform for illegal activity.
2. Ensure all funds originate from lawful sources.
3. Identify and mitigate fraud, corruption, and AML/WWFT risks.
4. Protect donors, beneficiaries, volunteers, and the Foundation's reputation.
5. Maintain ANBI status and compliance with regulatory requirements.
6. Ensure transparency and accountability in donation flows.

3. Scope

This Policy applies to:

- all Donors
- all Nonprofits
- all Users
- all financial transactions
- all hour registrations in the Time Bank
- all personnel, Board members, and contractors
- all platform operations and services

4. Principles

4.1 The Foundation maintains **zero tolerance** for:

- fraud
- corruption
- bribery
- money laundering
- terrorist financing
- misuse of funds
- falsification of data

4.2 All activities must support **public-benefit** objectives.

4.3 Integrity and transparency guide all financial decisions.

5. AML & Donor Due Diligence Checks

Before accepting significant Donations (threshold set at: **€2,500 or above**, or lower if risk indicators exist), the Foundation may conduct due diligence:

5.1 Basic Checks

- verify identity of the Donor
- verify organisation registration
- check against sanction lists (EU, UN, OFAC when relevant)
- confirm that funds come from legitimate sources

5.2 Enhanced Due Diligence (EDD)

Triggered if:

- the Donor is from a high-risk jurisdiction;
- the Donor refuses standard information requests;
- the Donor requests unusual conditions;
- the Donation is unusually large;
- the Donor is politically exposed (PEP).

EDD may include:

- source-of-funds documentation
- additional identity verification
- background checks
- review of corporate structure

5.3 Refusal of Donations

The Foundation will refuse Donations if:

- the source appears unlawful
- the donor appears on sanctions lists
- acceptance would violate public-benefit principles
- reputational or AML risks cannot be mitigated

6. Nonprofit Eligibility & AML Controls

To prevent diversion of funds:

6.1 Nonprofits must maintain valid ANBI/PBO/NGO status.
6.2 They must not be associated with:

- criminal activities
- extremist or terrorist groups
- corruption or political influence
- discriminatory or illegal operations

6.3 Nonprofits must provide identification information and cooperate with verification.

6.4 Funding may be withheld or reallocated if integrity concerns arise.

7. Fraud Prevention Measures

The Foundation employs:

7.1 Organisational Controls

- segregation of financial duties
- dual approval for payments
- transparent financial reporting
- periodic internal and external audits
- Board supervision

7.2 Platform Controls

- structured hour validation
- anomaly detection
- restrictions on user roles
- secure access protocols
- mandatory evidence for certain activities

7.3 User-Level Controls

- identity verification where needed
- Supervisor validation
- role-based access permissions
- reporting channels for misconduct

8. Detection of Suspicious Activity

Examples include:

- unusual hour spikes
- repeated duplicate entries
- Nonprofits refusing verification
- Donors pushing for irregular allocation
- transactions inconsistent with known activities
- attempts to obscure identity
- cash-like behaviour in digital systems
- manipulation of platform evidence
- unusually high or urgent donations without justification
- involvement of high-risk jurisdictions

Suspicious cases must be escalated immediately.

9. Reporting Obligations

9.1 Anyone (User, Employee, Nonprofit, Donor) may report concerns to:
integrity@burohelp.com

Reports may be anonymous.

9.2 Internal escalation is handled by the Director and the Treasurer.

9.3 If required under WWFT, the Foundation will report suspicious transactions to:
FIU-Nederland (Financial Intelligence Unit).

9.4 Reports are confidential and protected.

10. Investigation Procedures

10.1 Upon receiving a suspicion, the Foundation shall:

1. classify the issue (fraud, AML, compliance, misconduct);
2. freeze relevant accounts or allocations if necessary;
3. collect and review evidence;
4. cooperate with authorities when required;
5. document the process fully.

10.2 Investigations must be completed within:

- **30–90 days**, depending on complexity.

10.3 Findings are reviewed by the Board.

11. Suspension, Freezing, and Clawback

The Foundation may:

- suspend user accounts
- freeze donations
- suspend Nonprofit eligibility
- claw back misused funds
- block fraudulent hour entries
- refuse or return suspicious donations
- terminate Nonprofit participation
- notify donors of confirmed fraud
- notify authorities if required

12. Sanctions & Disciplinary Actions

Depending on severity, sanctions may include:

12.1 Against Users

- warnings
- permanent account removal
- reporting to Nonprofit / employer
- legal action if harm occurred

12.2 Against Nonprofits

- temporary suspension
- permanent removal
- recovery of misused funds
- reporting to authorities
- donor notification
- termination of funding agreements

12.3 Against Donors

- refusal of donations
- closing donor account
- legal reporting if illicit activity is suspected

12.4 Against Staff or Board Members

- disciplinary measures
- suspension
- dismissal
- legal reporting
- Board intervention

13. Training and Awareness

13.1 The Foundation provides AML and fraud-awareness training to the Board, Director, and relevant staff.

13.2 Nonprofits receive guidance on compliance obligations.

14. Confidentiality

14.1 All AML and fraud-related information must be handled with strict confidentiality.

14.2 Disclosure is permitted only when legally required or with explicit approval.

15. Recordkeeping

15.1 All AML and fraud-related records must be stored for **at least 7 years**, including:

- reports
- investigations
- audits
- suspicious activity logs
- actions taken

16. Policy Review & Amendments

16.1 This Policy shall be reviewed annually.

16.2 Amendments require Board approval.

17. Governing Law

This Policy is governed by the laws of the **Netherlands**, including WWFT and ANBI regulations.

18. Adoption & Signatures

Adopted by Stichting Burohelp on the 30th of November 2025