The Global Biodiversity Standard

Counter-Terrorist Financing Policy

October 2026

Status	Approved and in force
Version	1.1
Policy owner	CEO / designated Compliance Lead
Approved by	TGBS Ltd Board of Directors
Approval date	21 October 2026
Effective date	21 October 2026
Next review	October 2027: Annually, and after any material incident or legal change

The Global Biodiversity Standard (TGBS Ltd)

Counter-Terrorist Financing Policy

TGBS Ltd company policy

TGBS will prevent its funds, services, certification relationships and delivery channels from being used to support terrorism, sanctioned actors or prohibited activity, using proportionate risk assessment, screening and monitoring.

1. Purpose

Terrorist financing may involve legitimate as well as criminal funds and can occur through grants, contracts, suppliers, local partners, cash, assets or indirect support. TGBS will not knowingly make funds or economic resources available to a designated person or for terrorist purposes and will comply with applicable UK sanctions and counter-terrorism law.

This policy must be applied with the Anti-Fraud, Bribery and Corruption Policy, which contains TGBS's anti-money-laundering controls, and the Financial and Counterparty Due Diligence Policy.

2. Scope

This policy applies to TGBS Ltd directors, officers, employees, workers, consultants, contractors, volunteers and interns. It also applies, to the extent stated in contract or appointment terms, to TGBS hubs, certified assessors, technical reviewers, committee members, delivery partners and any other person acting for or representing TGBS.

- **Terrorist financing:** raising, providing, receiving, holding or using funds or economic resources for terrorism or a terrorist person or organisation, including facilitation or arrangements.
- **Designated person:** an individual or entity subject to an applicable asset freeze or financial sanction.
- **Economic resources:** assets of any kind that may be used to obtain funds, goods or services, including equipment, vehicles, access, training or other benefits.
- **Sanctions screening:** checking relevant names, ownership and control against applicable official lists, followed by investigation of possible matches.

3. Policy principles

TGBS will apply this policy lawfully, fairly, consistently and proportionately, with effective oversight, documented decisions and protection from retaliation.

4. Roles and responsibilities

- The Board approves the policy, oversees material risks and ensures that allegations involving senior leadership are handled independently.

- The CEO implements the policy, assigns proportionate controls and reports material matters to the Board. A responsibility may be delegated, but accountability remains with the role that delegated it.
- Directors and managers model the required conduct, act on concerns promptly, protect reporters from retaliation and identify conflicts before taking part in a decision.
- All covered persons must understand the policy, complete required training, keep accurate records and raise concerns without delay.
- Each hub must nominate a responsible lead, cascade relevant requirements to assessors and subcontractors, maintain suitable local controls, comply with applicable local law, and report material concerns to TGBS. A hub remains responsible for its own legal duties and personnel.
- Assessors and reviewers must act impartially, declare conflicts, protect evidence and information, and never allow commercial or relationship pressures to affect their professional judgement.
- The CEO acts as Compliance Lead unless the Board designates another competent person. Finance and contract owners must not release funds until required checks and approvals are complete.
- Hubs must know relevant payees, beneficiaries and subcontractors, control onward transfers, maintain evidence of delivery and report suspicious conduct or sanctions matches immediately.

5. Policy requirements

5.1. Risk assessment, screening and controls

- Assess country, counterparty, ownership/control, delivery chain, beneficiary, payment route, cash, diversion and security risks before approval and when circumstances change.
- Verify identity, legal status, beneficial ownership, bank account, purpose, source and destination of funds using reliable information.
- Screen counterparties, beneficial owners, key controllers and relevant payees against the UK Sanctions List and any other list legally applicable to the transaction. A name match must be resolved, not assumed.
- Use written budgets, permitted-use clauses, staged payments, evidence of expenditure and delivery, audit/information rights and restrictions on subgranting where risk requires.
- Avoid anonymous donations, unexplained third-party payments, personal accounts, unapproved cash, cryptocurrency and informal value-transfer systems. Any exceptional method requires enhanced due diligence and written approval.
- Re-screen before major payment and periodically for ongoing or higher-risk relationships; monitor changes in ownership, geography, activity and sanctions status.

5.2. Red flags

- secrecy, false or inconsistent identity information, opaque control or refusal to identify end users;
- a sanctioned/high-risk location, unusual routing, multiple intermediaries or payment unrelated to contract geography;
- unexplained cash withdrawals, rapid onward transfers, split payments, over-invoicing or goods that are difficult to verify;
- pressure to bypass checks, use another name/account or describe a transaction inaccurately;
- adverse information credibly linking a person, entity or controller to terrorism, sanctions evasion or violent groups.

6. Reporting and escalation

A person may raise a concern orally or in writing and may be accompanied or supported where appropriate. Anonymous reports will be considered as far as the available information allows. Reports should include the facts known, relevant dates, people involved and any evidence that can be preserved safely.

Situation	Route
Ordinary route	Report to the CEO and copy the Board Chair or another non-conflicted director.
Concern involves the CEO	Report to the Board Chair and at least one other non-conflicted director. The CEO must not receive, direct or decide the matter.
Concern involves the Board Chair	Report to the CEO and at least one other non-conflicted director. The Chair must not receive, direct or decide the matter.
Concern involves both the CEO and Chair, several directors, or internal independence is reasonably in doubt	Report to any non-conflicted director or to the Governance Contact, who must notify at least one other non-conflicted director and arrange an independent response. External professional advice or an external investigator must be used where necessary.
Immediate danger or suspected crime/regulatory breach	Contact emergency services, law enforcement or the relevant regulator where appropriate. Internal reporting is not a precondition.

The Board will maintain a current Policy Contact Register containing direct contact details for the CEO, Chair, Governance Contact and at least two other directors. The Governance Contact means the Company Secretary, if appointed, or a non-conflicted director designated by the Board.

No person may investigate, influence, decide or hear a review of a matter in which they are implicated or have an actual, potential or perceived conflict of interest. A report received by an implicated person must be forwarded immediately to a non-conflicted route without screening or alteration.

Retaliation, victimisation, obstruction, concealment, destruction of evidence and knowingly false or malicious allegations are prohibited. A report made honestly will not attract action merely because it is unsubstantiated.

7. Response and resolution

In the case of a potential match or suspicion:

1. Stop the transaction or internal processing without unlawfully dealing with the funds or economic resources.
2. Notify the Compliance Lead immediately through a conflict-free route and preserve records.
3. Do not alert the counterparty where doing so may be unlawful or prejudice an enquiry.
4. Obtain competent legal/banking advice, resolve false positives and make required reports to the Office of Financial Sanctions Implementation, National Crime Agency, police, bank or other authority.
5. Document the decision, licence or authority relied upon and any protective or contractual action.

8. Confidentiality and records

Information will be shared only with those who need it to protect people, assess the matter, comply with law, obtain advice or take action. Absolute confidentiality cannot be promised where disclosure is necessary for a fair process or legal duty.

Risk assessments, screening evidence, match resolution, payment monitoring, approvals and reports will normally be retained for at least six years, or longer where sanctions, banking, investigation, contract or legal requirements apply.

Personal data will be handled under the TGBS Data Protection Policy. Records must be factual, access-controlled and kept separately from general personnel or project files where sensitivity requires it.

9. Breaches and corrective action

TGBS may refuse or stop a transaction, restrict access, suspend work, terminate a relationship, freeze internal action pending lawful direction and report to competent authorities. It will not return, transfer or otherwise deal with funds where prohibited.

10. Monitoring and review

The CEO will review implementation and report material issues and trends to the Board. The policy will be reviewed on the date shown in the control table and sooner after a material incident, legal change or significant change to TGBS activities.

11. Related documents and legal framework

- TGBS Anti-Fraud, Bribery and Corruption Policy; Financial and Counterparty Due Diligence Policy; Whistleblowing Policy.
- Terrorism Act 2000; Sanctions and Anti-Money Laundering Act 2018; applicable UK counter-terrorism sanctions regulations and reporting duties; Proceeds of Crime Act 2002.