

Anti Bribery Modern Slavery and Human Rights Policy

Document control	Details
Version	2.0
Status	Approval-ready controlled policy - not effective or enforceable until documented approval and any required local implementation steps are complete
Intended Effective Date	The later of 1 September 2026 and the date of documented approval, subject to applicable local implementation requirements
Last Updated	1 October 2026
Supersedes	On effectiveness, Version 1.0 and the modern slavery and website-privacy text previously included in this document
Entity	TraCerLab SC, a private-law company specialising in traceability technologies, digital identification, mineral intelligence, data management and mining supply-chain compliance ("TraCerLab", "we", "us", or "our")
Registered Office	TraCerLab SC, Avenue Marcel Gourdin 60, 5001 Namur, Belgium; VAT BE0758359658 www.tracerlabgroup.com
Policy Owner	Legal and Compliance
Approval Authority	TraCerLab's governing body or a properly authorised delegate
Approval Evidence	Before effectiveness, the controlled copy must record the approving person or body, approval date, and decision or resolution reference
Contact	legal@tracerlabgroup.com
Classification	Public - corporate and client-facing

1. Purpose, status, and legal effect

TraCerLab prohibits bribery, corruption, modern slavery, human trafficking, forced labour, child labour, and related exploitation. We will not seek or retain business, obtain an advantage, accelerate an official action, reduce a lawful burden, or solve an operational problem through prohibited conduct.

This Policy establishes TraCerLab's global minimum rules for ethical business conduct, responsible business relationships, human-rights due diligence, reporting, investigation, and remediation. It is designed to protect people, TraCerLab, its customers and counterparties, and the integrity of public and private decision-making.

This Policy is a binding internal standard when adopted through the corporate, employment, consultation, notice, or workplace procedures required by applicable law. It binds directors, officers, employees, and other members of TraCerLab's workforce to the extent permitted by law and their governing terms. It binds a contractor, supplier, intermediary, customer, partner, joint venture, or other third party only where this Policy or equivalent requirements are incorporated into an agreement, code, onboarding condition, or other enforceable commitment.

Publication alone does not amend an employment agreement, collective agreement, customer agreement, supplier agreement, or applicable work rules. Nothing in this Policy:

- authorises conduct prohibited by law;

- removes a non-waivable right or remedy;
- creates a lawful basis for processing Personal Data;
- transfers a statutory duty from the person or entity on whom the law places it;
- guarantees that every violation will be prevented or detected; or
- creates third-party beneficiary rights beyond those arising under mandatory law or an express agreement.

Where a contract, local policy, or applicable law imposes a stricter requirement, the stricter requirement applies. Where requirements genuinely conflict, Covered Persons must stop, preserve relevant information, and obtain instructions from Legal before acting. No commercial objective, instruction, custom, urgency, seniority, or anticipated loss of business overrides this Policy.

2. Scope

2.1 People and entities covered

This Policy applies to:

- TraCerLab's governing-body members, directors, officers, employees, temporary staff, agency workers, interns, and secondees (collectively, "Personnel");
- controlled entities and business units, subject to local-law implementation requirements;
- any person acting for or on behalf of TraCerLab, including agents, consultants, introducers, lobbyists, customs brokers, freight or logistics intermediaries, sales representatives, and other intermediaries, to the extent an employment, agency, onboarding, or contractual instrument binds that person to this Policy or equivalent duties; and
- suppliers, subcontractors, professional advisers, consortium members, joint-venture partners, customers, and other counterparties to the extent required by their agreements or applicable law.

Personnel and persons acting for or on behalf of TraCerLab who are bound as described above are referred to together as "Covered Persons". The responsible relationship owner must ensure the required binding instrument is in place before an external person begins acting for or on behalf of TraCerLab. TraCerLab seeks risk-appropriate equivalent commitments from other Business Partners.

2.2 Activities covered

This Policy applies to all TraCerLab business activities, including:

- sales, marketing, procurement, tenders, licences, permits, inspections, taxes, customs, and regulatory interactions;
- gifts, hospitality, travel, entertainment, donations, sponsorships, community benefits, political activity, lobbying, recruitment, internships, discounts, credits, and other advantages;
- engagement and oversight of Business Partners;
- investments, acquisitions, joint ventures, consortiums, integrations, and material transactions;
- development, provision, configuration, or use of TraCerLab's current and future websites, software, services, features, support, and other offerings (collectively, the "Services"); and
- TraCerLab's own operations and upstream and downstream business relationships to the extent relevant to an identified risk or applicable duty.

2.3 Geographic application

This Policy is global. It applies even where prohibited conduct is locally tolerated, described by another name, or performed outside the country in which TraCerLab or a customer is established. Local addenda may impose additional controls but may not weaken the core prohibitions.

3. Core commitments

TraCerLab will:

- prohibit direct and indirect public-sector and private-sector bribery, kickbacks, facilitation payments, and corrupt influence;
- maintain risk-based procedures proportionate to TraCerLab's activities, markets, counterparties, and legal exposure;
- conduct risk-based due diligence before and during relevant business relationships;
- keep complete, accurate, and sufficiently detailed books, records, approvals, and supporting evidence;
- prohibit modern slavery and respect internationally recognised human rights;
- identify and assess actual and potential adverse impacts in TraCerLab's operations and relevant business relationships;
- prevent or mitigate potential impacts, cease or minimise actual impacts, use leverage responsibly, and contribute to remediation where TraCerLab caused or contributed to harm;
- provide and communicate safe routes for advice and concerns, subject to law and operational availability;
- prohibit retaliation against protected reporters, participants, and persons who refuse prohibited conduct;
- triage concerns and investigate appropriate matters fairly, independently, confidentially, and proportionately;
- apply lawful and proportionate corrective action, including discipline or termination where justified;
- train relevant people according to their roles and risk exposure;
- monitor effectiveness and improve controls after incidents, material changes, and periodic review; and
- make only accurate, supportable public statements about our programme, Services, supply chains, performance, and impact.

These commitments require an operating compliance programme. The existence of this Policy does not, by itself, prove that procedures are adequate or effective.

4. Definitions

For this Policy:

Adverse Human-Rights Impact means an action or omission that removes or reduces a person's ability to enjoy an internationally recognised human right.

Anything of Value includes money and any financial or non-financial benefit, regardless of amount. Examples include gifts, meals, entertainment, travel, accommodation, services, discounts, rebates, commissions, loans, debt relief, charitable or political contributions, sponsorships, confidential information, preferential treatment, employment, internships, secondments, contracts, licences, permits, visas, invitations, awards, and benefits provided to a relative, associate, or favoured organisation.

Associated Person means a person who performs services for or on behalf of TraCerLab, assessed by the actual circumstances and applicable law rather than title alone.

Bribe means offering, promising, authorising, giving, requesting, agreeing to receive, or accepting Anything of Value, directly or indirectly, to induce, reward, secure, or conceal improper performance, abuse of entrusted power, breach of duty, or improper influence. A bribe may benefit the decision-maker or another person and need not be paid, accepted, successful, or of substantial value.

Business Partner means a supplier, contractor, subcontractor, adviser, agent, intermediary, reseller, distributor, consultant, customer, consortium member, joint-venture participant, investee, acquisition target, or other business counterparty.

Child means a person under 18. **Child Labour** means work prohibited by the applicable legal minimum-age or hazardous-work rules, together with any higher standard expressly adopted in a controlled TraCerLab procedure or incorporated into the relevant agreement, including the worst forms of child labour. It does not include lawful, age-appropriate work that does not interfere with education, health, safety, or development.

Conflict of Interest means a situation in which personal, family, political, financial, or other interests could influence, or reasonably appear to influence, a person's independent judgment or duties.

Corruption means abuse of entrusted power for private gain or another improper purpose. It includes bribery, kickbacks, corrupt influence, embezzlement, misappropriation, bid manipulation, and concealment of those acts.

Facilitation Payment means an unofficial payment or benefit intended to secure or accelerate a routine action to which the payer is already entitled. It does not include a published, lawful fee paid directly to the responsible authority through an authorised method and supported by an official receipt.

Forced Labour means work or service exacted from a person under threat of a penalty and for which the person has not offered themselves voluntarily, subject to the narrow exceptions recognised by applicable law and international labour standards.

Government Entity includes a national, regional, local, municipal, indigenous, traditional, or other public authority; a regulator, ministry, agency, court, customs or tax authority; a public international organisation; and an entity owned, controlled, or performing a public function on behalf of the state.

Human Trafficking means recruiting, transporting, transferring, harbouring, or receiving a person through prohibited means for exploitation, as defined by applicable law. For a child, applicable law may not require proof of those means.

Kickback means returning or directing part of a payment or advantage as a reward for awarding or retaining business or providing another improper benefit.

Modern Slavery includes slavery, servitude, Forced Labour, debt bondage, Human Trafficking, forced or servile marriage, the worst forms of Child Labour, and other slavery-like practices recognised by applicable law.

Public Official includes:

- an elected, appointed, employed, contracted, or honorary officer or worker of a Government Entity;
- a person exercising a legislative, administrative, judicial, military, regulatory, customs, tax, licensing, inspection, public-procurement, or other public function;
- an officer, employee, or representative of a state-owned, state-controlled, or public-function enterprise, public university, public hospital, sovereign wealth fund, or public international organisation;
- a political party, party official, candidate for office, member of a royal family acting in an official capacity, or person holding a traditional or community authority role with public influence; and
- a person acting at the direction of, as an intermediary for, or for the benefit of any of the above.

When status is uncertain, Covered Persons must treat the person as a Public Official until Legal confirms otherwise.

Retaliation means a threatened, attempted, or actual adverse action linked to protected reporting, participation, cooperation, refusal, or remedy. It can include dismissal, demotion, reduced work, discipline, intimidation, harassment, threats, blacklisting, discrimination, adverse references, contract termination, or harm to a relative or associate.

5. Legal and standards framework

5.1 Applicable law

TraCerLab and Covered Persons must comply with all anti-bribery, anti-corruption, books-and-records, fraud, public-procurement, sanctions, anti-money-laundering, labour, trafficking, child-protection, whistleblowing, privacy, employment, and human-rights laws that apply to the relevant person, entity, conduct, transaction, or territory.

Depending on the facts and legal nexus, relevant laws may include:

- the Belgian Criminal Code, as amended, including rules on public and private corruption and liability of legal persons;
- the Belgian law implementing protections for private-sector whistleblowers;
- the UK Bribery Act 2010 and associated statutory guidance;
- the United States Foreign Corrupt Practices Act and other applicable anti-corruption laws;
- applicable French anti-corruption requirements, including Sapin II programme duties where the statutory scope conditions are met;
- applicable national laws implementing international and regional anti-trafficking, labour, and public-procurement duties;

- the UK Modern Slavery Act 2015, Australian Modern Slavery Act 2018, Canadian Fighting Against Forced Labour and Child Labour in Supply Chains Act, and California Transparency in Supply Chains Act, in each case only where the relevant entity, activity, nexus, and threshold tests are met;
- the EU Corporate Sustainability Due Diligence Directive and implementing national law, the EU Forced Labour Regulation from its applicable date, and other mandatory human-rights due-diligence or product restrictions where TraCerLab's legal role is in scope;
- the EU Conflict Minerals Regulation, EU Batteries Regulation, United States conflict-minerals rules, import prohibitions, and other sector-specific trade or supply-chain regimes only where the relevant product, role, volume, jurisdiction, and effective-date conditions are met; and
- privacy, legal-privilege, employment, private-investigation, records, and reporting rules relevant to due diligence and investigations.

A law is listed for issue-spotting only. Listing it does not state that TraCerLab is within its scope for every activity, reporting period, or group entity. Legal must confirm scope based on current facts before TraCerLab claims compliance or files a mandatory report.

5.2 Standards and guidance

TraCerLab uses the following as risk-management benchmarks to the extent relevant:

- the United Nations Guiding Principles on Business and Human Rights;
- the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct;
- the OECD Due Diligence Guidance for Responsible Business Conduct;
- the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas;
- the OECD Good Practice Guidance on Internal Controls, Ethics and Compliance;
- the International Labour Organization's core labour standards, forced-labour indicators, child-labour standards, and fair-recruitment principles; and
- applicable governmental guidance on proportionate anti-bribery procedures and modern-slavery reporting.

These standards inform this Policy but do not become directly applicable legislation merely because they are listed.

6. Governance and accountability

6.1 Governing body and senior management

TraCerLab's governing body, or a properly authorised committee, provides top-level oversight. It must:

- approve this Policy and material changes through the required governance process;
- set and communicate a culture in which lawful conduct takes priority over revenue, speed, or hierarchy;
- assign appropriate authority, independence, access, and resources for implementation;
- receive proportionate information about material risks, allegations, investigations, remediation, programme testing, and legally required disclosures;
- challenge management where controls or resources are inadequate; and
- ensure that compensation and performance measures do not reward prohibited conduct or suppression of concerns.

Senior management is responsible for implementing the Policy in its area, modelling compliant conduct, supporting risk-based controls, escalating concerns, protecting reporters, and correcting weaknesses.

6.2 Legal and Compliance

The designated Legal and Compliance function, whether performed internally or by an authorised adviser, is responsible for coordinating:

- legal interpretation and advice;

- corruption and human-rights risk assessments;
- risk-based due diligence and approval standards;
- reporting intake, triage, investigation oversight, and remediation tracking;
- registers, controlled procedures, training content, monitoring, and reporting;
- review of high-risk transactions and public statements; and
- updates following legal, organisational, geographic, service, or risk changes.

Legal and Compliance must have a route to escalate material matters outside normal management lines where independence requires it.

6.3 Managers

Managers must:

- understand the risks in their activities and Business Partners;
- ensure required approvals and checks occur before commitment or payment;
- create an environment in which concerns can be raised without Retaliation;
- escalate suspected misconduct promptly and preserve relevant records;
- never investigate serious allegations informally or promise an outcome or anonymity; and
- support remediation and management accountability.

6.4 Covered Persons

Each Covered Person must:

- read, understand, and follow the parts of this Policy relevant to their role;
- complete assigned training and attestations;
- disclose Conflicts of Interest and request approval before a controlled activity;
- recognise and escalate red flags;
- refuse prohibited conduct even if it causes delay or loss of business;
- maintain accurate records and cooperate with lawful reviews; and
- report suspected violations or seek advice promptly.

6.5 Business Partners

Where required by contract or onboarding conditions, Business Partners must meet this Policy or equivalent standards, communicate applicable requirements to relevant personnel and approved subcontractors, retain supporting evidence, permit proportionate verification, report suspected breaches, protect reporters, and remediate confirmed harm.

TraCerLab will not represent that a Business Partner is bound by this Policy unless an enforceable basis exists.

7. Risk assessment

TraCerLab must maintain and apply a documented, risk-based approach. Its purpose is to identify where harm or misconduct is most likely or severe and to allocate controls accordingly; it is not to treat every person, country, or transaction as presenting the same risk.

Risk assessments should consider, as relevant:

- country, sector, service, transaction, public-interface, and procurement risk;
- the use, qualifications, ownership, reputation, connections, and compensation of intermediaries;
- government ownership or control, politically exposed persons, sanctions, adverse information, and beneficial ownership, subject to law;

- permits, customs, taxes, inspections, licences, grants, public funding, state benefits, or public contracts;
- unusually high commissions, contingent fees, cash, opaque payment routes, urgency, or non-standard terms;
- labour recruitment, subcontracting, migration, temporary work, remote work sites, security arrangements, accommodation, transport, and retention of identity documents;
- vulnerable groups, including children, migrants, displaced persons, low-literacy workers, minority groups, human-rights defenders, and people in conflict-affected or high-risk areas;
- severity, scale, scope, irremediability, likelihood, and TraCerLab's connection to a potential impact;
- the reliability and limits of available information; and
- previous allegations, incidents, audit findings, control failures, and remedial performance.

Risk assessments must be refreshed periodically and after material triggers such as entry into a new market, material service or business-model change, new public-sector interaction, acquisition or joint venture, significant Business Partner, credible allegation, enforcement development, or change in law.

Nationality, ethnicity, religion, disability, gender, union status, or another protected characteristic must never be used as a proxy for risk.

8. Absolute anti-bribery and anti-corruption rules

Covered Persons must not, directly or indirectly:

- offer, promise, authorise, give, request, agree to receive, or accept a Bribe or Kickback;
- make, solicit, or accept a Facilitation Payment;
- use a third party, relative, charity, company, account, digital asset, reimbursement, credit, or other route to do what TraCerLab could not lawfully do directly;
- reward or influence a decision through employment, an internship, a contract, a discount, a donation, information, or any other advantage;
- conceal a benefit, recipient, purpose, relationship, source of funds, or conflict;
- knowingly ignore, avoid learning about, or fail to stop, escalate, or take appropriate action within the person's authority when circumstances indicate a substantial risk of misconduct;
- falsify or omit information from due diligence, an approval request, declaration, invoice, expense, register, bid, certification, or record;
- retaliate against a person who refuses, reports, or assists with a concern; or
- approve, instruct, encourage, assist, conspire in, attempt, or conceal any prohibited conduct.

The prohibition covers public and private transactions. It applies whether the advantage is for the recipient or another person; whether it is paid before or after a decision; whether the recipient has formal authority; whether the conduct succeeds; and whether company funds, personal funds, or a third party are used.

No manager, customer, official, shareholder, governing-body member, or other person may waive or authorise a Bribe. A performance target, customer demand, competitive pressure, local custom, instruction, or fear of losing business is never a defence.

9. Public Officials and official interactions

Interactions with Public Officials present heightened legal and perception risk. Covered Persons must:

- have a legitimate, documented business or legal purpose;
- use authorised and transparent channels;
- comply with rules applicable to both TraCerLab and the recipient;
- provide complete and truthful information;

- avoid personal benefits, side arrangements, secrecy, or preferential treatment;
- obtain any required written pre-approval before providing Anything of Value;
- document material interactions, decisions, approvals, and expenditures proportionately; and
- escalate an unusual request, threat, conflict, or suspected misuse of authority.

The same controls apply when a benefit is directed to an official's relative, associate, political organisation, favoured charity, community body, or other designee.

9.1 Licences, permits, inspections, customs, taxes, and enforcement

Covered Persons must not pay or confer a personal benefit to influence a permit, clearance, inspection, valuation, assessment, enforcement decision, investigation, court process, or regulatory outcome. They must not submit false information, conceal relevant facts, or obtain confidential government information improperly.

Payments must be made to the legally entitled authority through an authorised method, against official documentation. A request to pay an individual, intermediary, unrelated entity, personal account, cash collector, or unverified channel must be stopped and escalated.

9.2 Public procurement

In a public procurement or tender, Covered Persons must not:

- obtain or use confidential bid, evaluation, budget, competitor, or decision information improperly;
- influence specifications or award criteria through an undisclosed or improper arrangement;
- collude, rotate bids, submit cover bids, divide markets, or coordinate competitively sensitive conduct;
- offer Anything of Value to a decision-maker or connected person;
- use an undisclosed agent, subcontractor, consortium member, or conflict;
- make a false exclusion, eligibility, capability, local-content, ownership, human-rights, or other certification;
- communicate outside authorised procurement channels where restricted; or
- destroy or alter records relevant to a procurement, challenge, audit, investigation, or exclusion decision.

Relevant convictions, exclusions, investigations, conflicts, and remedial measures must be disclosed when and to the extent legally or contractually required. Legal must review any uncertainty before a declaration is submitted.

10. Facilitation demands, extortion, and personal safety

Facilitation Payments are prohibited, regardless of amount or local custom.

A published fee for a legitimate expedited or routine service is permitted only if the fee is lawful, available on transparent terms, paid directly to the responsible authority through an authorised channel, and supported by an official receipt or equivalent evidence.

If a person reasonably believes there is an imminent threat of death, physical injury, unlawful detention, or other serious personal harm, personal safety takes priority. A payment or transfer made under genuine duress is not treated as an approved business practice or a precedent. The person must, as soon as safely possible:

- move to safety and obtain emergency help where appropriate;
- report the incident to Legal or an authorised manager;
- accurately record the amount, recipient, circumstances, and purpose;
- preserve available evidence without increasing danger; and
- cooperate with a risk and remediation review.

A payment reasonably made under an imminent threat to life, physical safety, or liberty will not itself be treated as a breach of this Policy when the person reports it as soon as safely possible and records it accurately. This protection does not represent that the payment is lawful in every jurisdiction, excuse concealment, or prevent any legally required notification or corrective action.

Threats to property, schedule, revenue, or commercial interests alone do not qualify as a personal-safety emergency. Legal should be consulted before acting whenever time and safety permit.

11. Gifts, hospitality, entertainment, and travel

11.1 General rule

A gift, meal, entertainment, travel, accommodation, event, or other business courtesy may be offered or accepted only when all of the following are true:

- it has a genuine, lawful, and documented business, cultural, or protocol purpose;
- it is reasonable, proportionate, infrequent, and appropriate to the relationship and location;
- it is not intended, and could not reasonably be perceived, to influence or reward a decision or breach a duty;
- it is not cash, a cash equivalent, a personal loan, an investment opportunity, or a redeemable personal benefit;
- it is not requested by the recipient and does not create an obligation;
- it is transparent and would withstand public, regulatory, customer, and audit scrutiny;
- it complies with the recipient's rules and applicable law;
- it is not split, repeated, routed through others, or misdescribed to avoid a threshold or approval;
- it receives any required written pre-approval; and
- it is recorded accurately in the applicable register and books, including items declined or returned where the controlled procedure requires it.

An amount below an internal threshold is not automatically permissible. Internal thresholds are approval controls, not safe harbours and not statements of legality.

11.2 Prohibited circumstances

Business courtesies are prohibited when connected to a pending or reasonably foreseeable:

- tender, contract award, renewal, pricing, claim, dispute, or audit;
- permit, licence, customs, tax, inspection, enforcement, or regulatory decision;
- vote, grant, funding, certification, valuation, or official recommendation;
- hiring, promotion, admission, or selection decision; or
- request for confidential information or preferential treatment.

Lavish, sexually oriented, unlawful, secret, repetitive, or personally inappropriate entertainment is prohibited.

11.3 Public Officials

No benefit may be provided to or for a Public Official unless Legal confirms in writing that it is lawful, legitimate, proportionate, permitted by the recipient's rules, and approved under the controlled procedure. A narrow ceremonial or protocol item may be permitted only after that review. Country, agency, tender, or recipient rules may impose a complete prohibition.

11.4 Travel and accommodation

TraCerLab may pay reasonable and necessary travel or accommodation only for a legitimate business purpose and under written controls. Where permitted:

- TraCerLab must pay providers directly where practicable; any exception requires written pre-approval and documented justification;
- class, route, duration, and accommodation must be proportionate;
- no side trips, leisure extensions, per diems beyond policy, or expenses for relatives or guests may be funded;
- cash reimbursements require exceptional justification and evidence; and

- the traveller may not select an unrelated payment recipient.

11.5 Unsolicited or impractical-to-return items

If refusal or return would be unsafe, unlawful, or cause a serious protocol offence, the recipient must disclose the item promptly and follow Legal's written direction, which may include return, surrender, donation, shared workplace use, or another documented disposition. Personal retention is not presumed.

12. Donations, sponsorships, community benefits, lobbying, and politics

12.1 Charitable donations and sponsorships

A charitable donation, sponsorship, grant, or community benefit must:

- have a legitimate, documented purpose aligned with approved objectives;
- be subject to risk-based due diligence on the recipient, ownership or control, relevant Public Official connections, intended beneficiaries, use of funds, and reputation;
- not be requested, directed, or controlled by a decision-maker in exchange for an advantage;
- be made under a written agreement where proportionate;
- be paid through an authorised route to the verified organisation, not an individual or unrelated account;
- contain appropriate use, reporting, audit, anti-bribery, human-rights, and repayment or termination protections; and
- be monitored and recorded accurately.

Humanitarian urgency may justify an accelerated review but not the abandonment of sanctions, diversion, safeguarding, or corruption controls.

12.2 Political contributions and activity

TraCerLab prohibits corporate political donations and partisan sponsorships globally. No TraCerLab funds, assets, Services, facilities, name, data, or working time may be given, loaned, discounted, or otherwise used as a political donation, partisan sponsorship, campaign contribution, in-kind support, fundraising assistance, or other partisan benefit for a political party, candidate, campaign, or political officeholder. This prohibition does not prevent legitimate arm's-length dealings with public bodies or Public Officials acting in an official capacity, which remain subject to Section 9. Lawful, non-partisan public-policy engagement, industry-association membership, and lobbying remain subject to Section 12.3 and must not be used to evade this prohibition.

Personnel may engage in lawful personal political activity in their own capacity, on their own time and at their own expense. They must not imply TraCerLab endorsement, use confidential information, coerce colleagues or Business Partners, seek reimbursement, or allow the activity to create an undisclosed Conflict of Interest.

12.3 Lobbying and advocacy

Lobbying, public-policy engagement, and advocacy on TraCerLab's behalf must be lawful, transparent, factually accurate, authorised, and documented. Required registrations and disclosures must be completed. No person may use lobbying, an industry association, a consultant, or grassroots activity to conceal a payment, source, client, or decision-maker benefit.

13. Conflicts of interest, hiring, and personal relationships

Covered Persons must disclose an actual, potential, or perceived Conflict of Interest promptly and before participating in a relevant decision. Disclosure does not necessarily prohibit the activity, but the conflict must be assessed and managed through measures such as recusal, independent review, reassignment, divestment, information barriers, approval, or termination of the conflicting arrangement.

Examples include:

- a financial or ownership interest in a Business Partner or competitor;
- a family, romantic, household, political, or close personal relationship with a decision-maker;

- outside employment, board service, public office, advisory work, or investment;
- supervision, selection, payment, or evaluation of a connected person;
- accepting an opportunity learned through a TraCerLab role; and
- receiving a personal benefit tied to a TraCerLab decision.

Employment, internships, secondments, scholarships, contracts, references, or work experience must never be offered or withheld to influence a Public Official or private counterparty. Candidates connected to a decision-maker require independent, merit-based assessment, disclosure, and written approval under the controlled procedure.

14. Business Partner due diligence and management

14.1 Risk-based review

Before engagement, renewal, material expansion, or a significant payment, the responsible owner must ensure that the required level of due diligence is complete and that unresolved red flags have been escalated. The depth of review must reflect the actual risk and may include, where lawful and proportionate:

- identity, legal existence, address, ownership, control, and beneficial ownership;
- qualifications, experience, resources, reputation, references, and commercial rationale;
- Public Official, political, customer, employee, family, or other relevant connections;
- sanctions, debarment, enforcement, litigation, adverse media, and misconduct history;
- source and destination of funds and proposed banking arrangements;
- compensation, commissions, discounts, success fees, expenses, and whether they are reasonable for documented services;
- use of subcontractors, subagents, recruiters, labour brokers, or other intermediaries;
- anti-bribery, labour, recruitment, safeguarding, grievance, privacy, security, and recordkeeping controls;
- actual or potential Adverse Human-Rights Impacts and capacity to prevent or remediate them; and
- the Business Partner's explanation and evidence addressing identified red flags.

Due diligence must be evidence-based and documented. Screening alone is not sufficient, and the absence of a database match is not proof of integrity.

14.2 Contractual controls

Risk-appropriate written terms may require:

- compliance with applicable law and this Policy or equivalent standards;
- accurate representations and continuing disclosure of material changes;
- a defined scope, deliverables, compensation, payment route, and prohibition on unauthorised subagents;
- anti-bribery, modern-slavery, fair-recruitment, child-protection, recordkeeping, privacy, and reporting duties;
- training or certification where proportionate;
- flow-down to approved subcontractors;
- access to relevant records and proportionate audit or assessment rights;
- prompt notification, cooperation, corrective action, and remediation;
- suspension, withholding, repayment, indemnity, or termination rights where lawful; and
- preservation of rights to report suspected criminal conduct or protect affected people.

Contract language does not replace due diligence, monitoring, or commercial oversight.

14.3 Payments

Payments must correspond to legitimate, documented goods or services that have been provided, delivered, or otherwise become contractually due; be reasonable and consistent with the agreement; be supported by a sufficiently detailed invoice or equivalent evidence; and be made to the verified contracting party through an authorised account in an appropriate jurisdiction. A documented and approved advance may be paid only when the contract permits it, the commercial rationale is clear, risk-appropriate safeguards are in place, and later reconciliation is required.

The following require escalation before payment:

- cash, digital assets, bearer instruments, gift cards, or other difficult-to-trace value;
- payment to a personal, employee, official, unrelated, nominee, or third-party account;
- payment in a country unrelated to the work or contracting party;
- advance, round-sum, duplicate, accelerated, success-based, or unusually high payment;
- vague descriptions such as "special services", "facilitation", "miscellaneous", or "relationship management";
- unexplained tax, customs, community, security, permit, or government-related charges;
- splitting, backdating, side letters, over-invoicing, under-invoicing, or requests to omit information; and
- a payment requested after a red flag, concern, or incomplete deliverable.

14.4 Monitoring and renewal

Relationship owners must monitor performance and risk proportionately. Due diligence must be refreshed on a risk-based cycle and when ownership, management, scope, geography, compensation, subcontracting, allegations, sanctions status, or other material circumstances change.

A Business Partner must not be retained merely because termination would be inconvenient. Equally, disengagement must be responsible where abrupt termination could worsen an Adverse Human-Rights Impact. Legal must coordinate any suspension, remediation, or exit.

14.5 Acquisitions, investments, and joint ventures

TraCerLab will apply proportionate anti-corruption and human-rights due diligence to acquisitions, investments, joint ventures, consortiums, and similar transactions. Controls should address ownership, government connections, historic conduct, liabilities, labour practices, Business Partners, books and records, contractual protections, governance rights, integration, remediation, and post-closing review.

If pre-completion diligence is restricted, the limitation and residual risk must be documented, protective terms used where possible, and priority post-completion review and remediation planned. No transaction structure may be used to evade this Policy.

15. Financial controls, books, and records

TraCerLab requires books and records that are accurate, complete, timely, and sufficiently detailed to show the true nature, purpose, amount, recipient, approval, and business rationale of a transaction.

Covered Persons must not:

- create or use an off-book account, slush fund, undisclosed asset, or unrecorded liability;
- make a false, misleading, incomplete, vague, or disguised entry;
- approve or pay a sham, inflated, duplicate, altered, or unsupported invoice;
- misclassify a gift, commission, donation, sponsorship, travel cost, government fee, community payment, refund, credit, or rebate;
- use a personal account, personal card, expense reimbursement, credit note, barter, or non-cash transfer to bypass controls;
- split a transaction to avoid review or approval;
- backdate, destroy, alter, fabricate, or conceal a record; or

- pressure another person to approve, certify, or record information they know or suspect is inaccurate.

Approval must be substantive, not automatic. An approver must have sufficient authority, independence, information, and time to assess the request. The requestor and approver must be separated where the controlled procedure requires it.

Suspected errors must be corrected transparently through authorised accounting processes, preserving the original entry and audit trail where required. Records are retained under applicable schedules and legal holds; they must not be destroyed when an investigation, audit, dispute, request, or proceeding is pending or reasonably anticipated.

16. Modern slavery and human-rights commitments

16.1 Respect for human rights

TraCerLab respects internationally recognised human rights. We prohibit Modern Slavery in our operations and do not knowingly cause, contribute to, facilitate, conceal, or benefit from it. We expect Business Partners to meet equivalent standards and to address risks in their own operations and relevant business relationships.

Our approach is guided by the responsibility to:

- avoid causing or contributing to Adverse Human-Rights Impacts;
- prevent or mitigate impacts directly linked to TraCerLab's operations, Services, or business relationships, even where TraCerLab did not cause them;
- cease, prevent, or minimise conduct causing or contributing to harm;
- use and build leverage responsibly;
- enable or cooperate in legitimate remediation where appropriate; and
- communicate how material impacts are addressed, subject to safety, privacy, privilege, and legal restrictions.

Risk-based prioritisation is permitted when not all impacts can be addressed at once. Priority must be based primarily on severity and likelihood, not commercial value, publicity, or ease of response. Prioritisation does not remove the responsibility to address lower-priority impacts over time.

16.2 Fundamental labour standards

TraCerLab prohibits:

- Forced Labour, slavery, servitude, debt bondage, Human Trafficking, and the worst forms of Child Labour;
- violence, threats, intimidation, coercion, deception, abduction, or abuse of vulnerability;
- charging or passing recruitment fees or related costs to a worker for obtaining work performed for TraCerLab, and any equivalent practice prohibited by applicable law or an incorporated standard;
- confiscation, destruction, concealment, or denial of access to passports, identity documents, permits, bank cards, or other personal property, except narrowly where law requires temporary handling and the worker has free, prompt access;
- withholding wages, deposits, or benefits to compel work or prevent departure;
- restrictions on lawful freedom of movement or resignation;
- misleading terms, contract substitution, undisclosed deductions, or work materially different from what was agreed;
- excessive or involuntary overtime, unsafe working or living conditions, or denial of legally required rest;
- unlawful discrimination, harassment, retaliation, or interference with lawful freedom of association and collective bargaining; and
- purchasing practices knowingly designed to make compliance with applicable wage, hour, safety, or labour obligations infeasible.

Workers must receive understandable information about material employment terms before work begins and, where relevant, before migration. Wages and legally required benefits must be paid accurately and on time. Work must be freely chosen, and workers must be able to leave employment subject only to lawful, reasonable notice.

16.3 Children and young workers

No person may be employed below the minimum age required by applicable law or any higher minimum expressly adopted in a controlled TraCerLab procedure or incorporated into the relevant agreement. No person under 18 may perform hazardous work or work likely to harm health, safety, morals, education, or development.

Age verification must be lawful, proportionate, respectful, and designed not to exclude people merely because standard documents are unavailable. If Child Labour is identified, the response must prioritise the child's best interests, safety, education, family circumstances, and protection from loss of necessary support or displacement into more dangerous work. Immediate dismissal without a child-centred remediation plan may increase harm and is not the default response.

16.4 Recruitment and migrant workers

Recruitment must be transparent and free from coercion and deceptive practices. Recruiters and labour brokers require risk-based due diligence and oversight. TraCerLab will use risk-appropriate contractual and oversight measures to extend the employer-pays principle to workers supplied through Business Partners. Where a worker has paid a prohibited recruitment fee or related cost, the responsible entity must support prompt, verifiable repayment consistent with law and a worker-centred remedy plan.

Migrant, temporary, agency, contract, and informal workers must receive protections equivalent to those required by applicable law, without unlawful discrimination. Immigration status or dependency on an employer must not be used to suppress a concern or compel work.

16.5 Security and community impacts

Security arrangements, whether public or private, must respect human rights and use force only as permitted by law and proportionate to a legitimate need. Credible allegations of violence, exploitation, unlawful detention, sexual abuse, or retaliation connected to security personnel require urgent escalation.

Engagement with local, indigenous, traditional, or affected communities must be lawful, culturally appropriate, and free from coercion or corrupt influence. Community payments or benefits must follow Sections 9 and 12 and must not be used to bypass rights, consent, consultation, or public-procurement requirements.

17. Human-rights due diligence

TraCerLab must implement and maintain risk-based, ongoing human-rights due diligence proportionate to its size, activities, leverage, and connection to potential harm.

17.1 Identify and assess

TraCerLab will seek to identify and assess actual and potential impacts through appropriate sources, which may include:

- internal operational information and worker or Business Partner feedback;
- contract, recruitment, payroll, working-time, safety, grievance, and audit evidence;
- country, sector, commodity, conflict, migration, and recruitment-risk information;
- credible civil-society, trade-union, community, expert, government, and international-organisation sources;
- allegations, grievances, adverse media, legal proceedings, enforcement actions, and whistleblowing reports;
- customer or supplier information, subject to lawful use and verification; and
- engagement with potentially affected people or legitimate representatives where safe and practicable.

TraCerLab will not rely solely on questionnaires, certifications, database screening, remote technology, or contractual assurances when the risk warrants further review.

17.2 Meaningful engagement

Engagement should be accessible, safe, culturally and linguistically appropriate, and sensitive to power imbalance, gender, disability, literacy, age, migration status, and risk of retaliation. Participation must not be coerced. TraCerLab must not disclose a participant's identity to an employer, recruiter, authority, customer, or other person without a lawful basis and an assessment of safety and necessity.

Where direct engagement is unsafe or impracticable, TraCerLab may use credible representatives, experts, unions, worker organisations, community organisations, or other appropriate sources. Engagement is not meaningful if participants cannot speak freely or if it increases risk.

17.3 Prevent and mitigate

Depending on TraCerLab's connection and leverage, actions may include:

- changing a practice, specification, deadline, pricing structure, incentive, or purchasing decision;
- requiring a time-bound corrective-action plan with measurable ownership and milestones;
- providing guidance, training, resources, or collaborative support;
- increasing oversight, worker engagement, verification, or contractual protection;
- pausing an activity, onboarding, payment, deployment, or relationship;
- working with customers, peers, industry bodies, worker representatives, civil society, or authorities where lawful and safe; and
- responsibly disengaging as a last resort or when severe harm cannot otherwise be prevented.

A corrective-action plan must not be used to tolerate ongoing severe abuse. Immediate protective action may be required before a full investigation is complete.

17.4 Track effectiveness

Controls should be assessed using reliable qualitative and quantitative information. Measures may include completion and quality of due diligence, time to corrective action, recurrence, worker access to remedy, repayment of fees or wages, closure quality, training effectiveness, audit findings, and stakeholder feedback.

Metrics must be interpreted carefully. A low number of reports may indicate underreporting rather than low risk. Targets must not incentivise concealment, premature case closure, abrupt worker dismissal, or superficial audit performance.

17.5 Communicate

TraCerLab may communicate material due-diligence information through this Policy, legally required statements, contractual reporting, customer responses, or other appropriate channels. Communications must be accurate, supportable, current, and sufficiently specific to the reporting period and entity. They must protect affected people, reporters, legitimate confidentiality, security, privilege, and legal restrictions.

18. Conflict-affected, high-risk, and regulated supply chains

Where TraCerLab's own activity or a relevant business relationship involves a conflict-affected or high-risk area, a regulated material, or a supply chain subject to mandatory due diligence, TraCerLab will apply the requirements that actually govern its role and the relevant transaction.

Risk assessment may include:

- serious abuses associated with extraction, transport, trade, handling, or export;
- direct or indirect support to non-state armed groups or abusive public or private security forces;
- bribery, fraudulent misrepresentation, money laundering, tax or royalty evasion, and concealment of origin;
- forced or child labour, trafficking, unsafe work, displacement, sexual and gender-based violence, and attacks on human-rights defenders;
- corruption or coercion in licences, access rights, transport, checkpoints, inspections, taxation, community arrangements, or public procurement; and
- the reliability, provenance, completeness, and limitations of records and representations.

Where applicable, controls should reflect a five-step risk-based process: management systems; risk identification and assessment; risk response; independent audit where required; and public reporting where required.

TraCERLab will not state that a material, site, supplier, customer, transaction, or supply chain is "conflict-free", "slavery-free", "ethical", "compliant", or equivalent unless the defined criteria, evidence, scope, limitations, assurance, and legal basis support that specific claim. A record, certificate, platform entry, analytical output, or absence of a warning is not conclusive proof.

No statement in this section asserts that TraCERLab imports, places, produces, handles, or trades any particular regulated material or that a named statutory regime applies. Applicability must be verified against actual roles, products, thresholds, origin, destination, and reporting period.

19. Responsible design and use of the Services

The Services may support customers or authorised users in collecting, organising, reviewing, or communicating information relevant to business integrity or human-rights risks. They do not replace legal advice, worker engagement, independent investigation, statutory due diligence, or human judgment.

TraCERLab will never claim that a Service automatically proves the existence or absence of a violation, reaches a legal conclusion, or itself provides remedy. TraCERLab may make a narrowly defined claim that a feature helps surface a specified indicator only when the claim is objectively substantiated for its stated context and describes the validation population, material data dependencies, performance limitations, and potential false positives and false negatives. Indicators, alerts, scores, classifications, and analytical outputs may be incomplete or incorrect and must be reviewed by qualified people alongside contextual evidence before consequential action.

The Services must not knowingly be configured or used to:

- facilitate exploitation, corruption, retaliation, unlawful surveillance, discrimination, or worker blacklisting;
- expose a reporter, affected person, child, vulnerable worker, or human-rights defender to avoidable harm;
- replace a fair investigation with an automated conclusion;
- represent an unverified assertion as a legal finding or certification; or
- conceal, alter, or delete information to obstruct a lawful review or remedy.

Where TraCERLab becomes aware of a credible risk of prohibited use, it may investigate, restrict, suspend, preserve, disclose, or terminate access as permitted or required by law and the applicable agreement. Any response must consider safety, evidence preservation, privacy, due process, and the risk that abrupt action could worsen harm.

20. Advice, speaking up, and external reporting

20.1 When to seek advice or report

Covered Persons should seek advice before acting when a situation is unclear. They must report promptly when they know or reasonably suspect:

- a Bribe, Facilitation Payment, Kickback, corrupt influence, conflict, false record, or control circumvention;
- Modern Slavery, Human Trafficking, Child Labour, Forced Labour, abusive recruitment, document retention, violence, or retaliation;
- an attempt, request, pressure, instruction, concealment, or threat connected to prohibited conduct;
- a Business Partner red flag that has not been resolved;
- destruction or alteration of relevant evidence;
- misuse of a Service to facilitate or conceal harm; or
- Retaliation against a reporter, witness, affected person, or person who refused misconduct.

No person is expected to investigate before reporting. A reasonable concern may be reported even if evidence is incomplete or the reporter is unsure which law or policy applies.

20.2 Internal channels

Concerns and requests for advice may be sent to legal@tracerlabgroup.com or through another verified channel formally communicated by TraCERLab. Privacy concerns may also be sent to privacy@tracerlabgroup.com.

Before this Policy takes effect, the Policy Owner must verify that each published channel is active, tested, access-controlled, assigned to authorised case owners, supported by documented escalation and absence-cover arrangements, and capable of meeting applicable privacy and response requirements. A channel must not be published or left in this Policy if those conditions are not met.

The Policy Owner must also document, for each relevant TraCerLab entity, whether a statutory internal reporting channel is required. Where the Belgian private-sector whistleblower law or another regime applies, the designated procedure and channel must be operational before effectiveness and must support the legally required reporting methods, independence, confidentiality, consultation, acknowledgements, feedback, records, information about external reporting, and anonymous reporting where required or formally offered. A general email address does not, by itself, satisfy those duties.

A person need not report to someone implicated in, controlling, or conflicted by the matter. A manager who receives a concern must preserve confidentiality, avoid substantive fact-finding unless authorised, and escalate it promptly through an appropriate independent route.

TraCerLab will accept anonymous information where lawful and technically available, but it cannot guarantee anonymity or two-way follow-up. Confidentiality will be protected to the extent reasonably possible and lawful; information may need to be shared on a need-to-know basis to protect people, investigate fairly, obtain advice, or comply with law.

20.3 External channels and emergency help

Nothing in this Policy requires internal reporting before a person contacts a competent regulator, law-enforcement body, labour inspectorate, ombudsperson, court, trade union, legal adviser, recognised whistleblowing authority, or other protected external channel. Nothing restricts a legally protected disclosure or cooperation with an authority.

Where someone faces immediate danger, emergency services or an appropriate local protection organisation should be contacted where safe. A person should consider the risk of retaliation or further harm before alerting an alleged exploiter or an authority that may be implicated.

TraCerLab does not offer legal, immigration, medical, or emergency-protection services through the reporting email address.

20.4 Non-retaliation

TraCerLab prohibits Retaliation against a person who:

- reports information they reasonably believe is true at the time;
- seeks advice or raises a question about possible misconduct;
- refuses to pay a Bribe, exploit a person, falsify a record, or engage in other prohibited conduct;
- participates in or supports a review, investigation, hearing, or remedy; or
- makes a legally protected disclosure externally.

Protection applies even if the concern is not substantiated. Knowingly making a materially false report or fabricating evidence is not protected and may result in lawful, proportionate action; an honest mistake, incomplete information, or inability to prove a concern is not a knowingly false report.

Retaliation concerns must be treated as separate potential violations and addressed promptly. A person must not be disadvantaged for losing or refusing business because compliance with this Policy required it.

20.5 Affected-person and stakeholder grievances

A whistleblowing route is not, by itself, an adequate grievance mechanism for a worker, child, community member, human-rights defender, or other potentially affected person. Where TraCerLab's risk profile, activity, contract, or applicable law requires it, TraCerLab will establish or participate in a distinct operational-level grievance process that is:

- legitimate, accessible, predictable, equitable, transparent about process, rights-compatible, and a source of continuous learning;
- available without charge through channels appropriate to language, literacy, disability, connectivity, geography, culture, and safety;

- open to affected people and, where appropriate, their legitimate representatives, trade unions, human-rights defenders, and relevant civil-society organisations;
- administered by people with suitable independence, competence, safeguarding awareness, and conflict controls;
- capable of confidential intake, status communication, dialogue, reasoned outcomes, review or escalation, remedy tracking, and non-retaliation protections; and
- designed through engagement with intended users where safe and practicable.

Using the process must be voluntary and must not block access to a court, regulator, labour inspectorate, trade union, national human-rights institution, arbitration, mediation, or another judicial or non-judicial remedy. TraCerLab will not require a person to waive a non-waivable right as a condition of raising a grievance or receiving an undisputed remedy.

The applicable procedure will state who can use it, its scope, available channels, indicative steps, confidentiality limits, escalation and review routes, and legally required acknowledgement or feedback periods. It must not publish a deadline or channel that is not operationally supported.

21. Triage, investigation, and fair process

TraCerLab will triage concerns and reports received promptly and proportionately, including an assessment of credibility, urgency, scope, conflicts, and materiality. The response may include immediate safeguarding, preservation of evidence, legal advice, interim controls, referral, investigation, remediation, and monitoring.

Investigations must be:

- authorised and scoped by an appropriate, sufficiently independent person;
- conducted by qualified people free from material conflicts;
- objective, proportionate, timely, and appropriately documented;
- respectful of the presumption of innocence, fair treatment, labour rights, privacy, privilege, and applicable local procedure;
- designed to protect reporters, witnesses, affected people, evidence, and the integrity of the process; and
- adjusted if new facts change risk, scope, or urgency.

No manager or colleague may conduct covert monitoring, search a personal device, access an account, interview witnesses, promise immunity, confront an alleged perpetrator, or collect sensitive evidence unless authorised and lawful. A person must not obstruct an investigation or delete, alter, coach, fabricate, or conceal evidence.

Interim measures are precautionary and do not determine guilt. They may include separating people, changing access, pausing a payment or activity, suspending a Business Partner, protecting a worker, or preserving records. Measures must be lawful, proportionate, and reviewed.

Information will be shared only as appropriate for safety, investigation, remediation, governance, advice, insurance, audit, contractual duties, or legal requirements. TraCerLab will not promise a reporter a particular outcome, complete secrecy, or disclosure of confidential disciplinary action.

Where reporting to an authority is considered, TraCerLab will assess applicable duties, privilege, safety, victim interests, reporting protections, self-reporting incentives, and the risk that disclosure could cause additional harm. Mandatory reporting obligations prevail.

22. Remediation and consequences

22.1 Corrective action

Where a concern is substantiated or a control fails, TraCerLab will select lawful and proportionate measures based on severity, involvement, intent, cooperation, history, harm, legal duties, and remediation needs. Measures may include:

- immediate protection or support for an affected person;
- stopping or changing an activity, decision, payment, access, incentive, or control;

- correcting records, recovering funds, repaying prohibited fees or withheld wages, or returning identity documents;
- a corrective-action plan, training, supervision, reassignment, warning, discipline, or dismissal;
- suspension, withholding, audit, repayment, contractual claim, or termination of a Business Partner;
- notification to a customer, insurer, auditor, regulator, authority, or other person where lawful and required;
- cooperation with a legitimate investigation or remedy process; and
- root-cause analysis and programme improvement.

Seniority, revenue, performance, or relationship value does not shield a person from consequences. Managers may be held accountable for directing misconduct, ignoring red flags, suppressing concerns, retaliating, or failing to implement assigned controls.

22.2 Human-rights remedy

Where TraCerLab caused an Adverse Human-Rights Impact, it will provide for or cooperate in remediation as appropriate. Where it contributed, it will cease or prevent its contribution and use leverage to mitigate remaining harm, while contributing to remedy proportionate to its involvement. Where an impact is directly linked through a business relationship without TraCerLab causing or contributing, TraCerLab will use or seek to increase leverage and support a legitimate response appropriate to the circumstances.

Remedy should be informed by affected people and may include restitution, compensation, repayment, rehabilitation, satisfaction, apology, guarantees of non-repetition, restoration of employment or documents, access to services, or another appropriate measure. A remedy must not require a person to waive non-waivable rights or remain silent about unlawful conduct. Any settlement, confidentiality term, or release requires Legal review and must comply with law.

22.3 Responsible disengagement

Suspension or termination may be necessary where severe harm is occurring, a Business Partner refuses remediation, leverage is ineffective, or continuing the relationship would be unlawful. Before disengaging where time permits, TraCerLab should assess foreseeable effects on workers and affected communities, communicate expectations, preserve evidence, seek to prevent retaliation, and plan measures that reduce additional harm.

Commercial continuity does not justify ongoing severe abuse. Conversely, abrupt exit must not be used as a substitute for remedy where TraCerLab caused or contributed to harm.

23. Training and communication

TraCerLab must assign training according to role and risk.

The programme must include, to the extent applicable and risk-appropriate:

- induction for relevant Personnel;
- periodic refresher training;
- enhanced scenario-based training for governing-body members, managers, sales, procurement, finance, government-facing roles, field or operations roles, investigators, product teams, and relationship owners;
- tailored communication for Business Partners and workers where contract, risk, language, literacy, or access requires it;
- practical instruction on red flags, approvals, records, refusal, escalation, non-retaliation, safeguarding, and emergency response;
- knowledge checks, attestations, attendance records, and follow-up for non-completion; and
- evaluation of whether training changes knowledge and behaviour.

Training must reflect local requirements and be understandable to the intended audience. Completion records show participation, not necessarily competence or programme effectiveness.

24. Monitoring, assurance, and continuous improvement

TraCerLab will monitor and review the programme proportionately. Methods may include:

- periodic risk-assessment refreshes;
- testing approvals, registers, transactions, due-diligence files, and contractual controls;
- targeted review of high-risk payments, intermediaries, recruitment practices, or procurement activity;
- confidential feedback, worker or stakeholder engagement, and grievance analysis;
- investigation and root-cause findings;
- internal or independent assurance where justified;
- review of corrective actions and recurrence;
- governance reporting using balanced, contextualised measures; and
- benchmarking against relevant legal guidance and responsible-business standards.

Testing must examine design and operation. The fact that a document, clause, training module, screening result, certification, or technical feature exists is not proof that a control works.

Material weaknesses must have an owner, risk rating, action, target date, escalation route, and evidence of closure. A target date must not be represented as a completed control.

The Policy and supporting procedures must be reviewed at least annually and sooner after a material legal change, incident, control failure, business change, service change, market entry, acquisition, or stakeholder finding.

25. Annual modern-slavery and supply-chain statements

This Policy is not an annual modern-slavery statement for a specific entity or financial year.

Before publishing or filing a mandatory or voluntary statement, TraCerLab must verify:

- the reporting entity or entities, group structure, jurisdiction, threshold, and reporting period;
- the applicable deadline, registry, website-link, language, board or governing-body approval, and signature requirements;
- the organisation's actual structure, operations, and supply chains during that period;
- the risks identified and the methodology and evidence supporting them;
- the steps actually taken during the period, including due diligence, remediation, training, engagement, and effectiveness assessment;
- any identified gaps, limitations, incidents, and planned actions, clearly distinguished from completed actions; and
- consistency with contracts, audit evidence, regulatory filings, public claims, and prior statements.

A statement must be approved and signed by the person or body required by the applicable law. An undated template, future commitment, general policy, or technology description must not be presented as a completed statutory statement. If no steps were taken in a required reporting period and the law permits that disclosure, the statement must say so accurately rather than imply otherwise.

Voluntary statements must be clearly identified as voluntary and must not imply statutory scope, regulator approval, independent assurance, or legal compliance that has not been verified.

26. Privacy, confidentiality, and records

26.1 Controlling privacy notice

Personal Data handled under this Policy is governed by the TraCerLab Global Privacy Policy and Data Protection Notice, applicable workforce or recruitment notices, customer instructions, data processing agreements, and any required local or activity-specific notice.

The current master public notice is the TraCerLab Global Privacy Policy and Data Protection Notice.

That notice, together with any more specific lawful notice or agreement, controls over any privacy summary in this Policy. This document does not duplicate website, Service, workforce, whistleblowing, investigation, or Business Partner privacy disclosures and must not be used as a substitute for them.

Privacy questions and requests may be sent to privacy@tracerlabgroup.com.

26.2 Due diligence, reporting, and investigation data

TraCerLab must process Personal Data for due diligence, conflicts, reporting, safeguarding, investigations, remediation, monitoring, and legal compliance only when there is an appropriate role, purpose, lawful basis, and-where required-condition for sensitive or criminal-offence data. For each material processing activity under this Policy, the accountable owner must ensure that TraCerLab's internal records identify the applicable controller or processor role, purpose, lawful basis, data categories, recipients, retention, international transfers, and any required data protection impact assessment.

Processing must be:

- necessary and proportionate to the identified purpose and risk;
- limited to relevant, reliable, and reasonably current information;
- subject to appropriate accuracy, access, confidentiality, security, retention, and deletion controls;
- transparent through an applicable notice unless a lawful, documented restriction or exception applies;
- designed to prevent unauthorised retaliation, discrimination, profiling, or disclosure;
- conducted with additional safeguards for children, vulnerable people, reporters, witnesses, allegations, criminal-offence data, biometrics, precise location, identity documents, and other sensitive information; and
- shared only with recipients that have a lawful need and appropriate protections.

Unverified allegations must be identified as such and not presented as established fact. Access must be restricted according to role and need. Records must not be retained indefinitely merely because they relate to compliance; applicable schedules, legal holds, limitation periods, statutory duties, safety, and remedy needs determine retention. Where a fixed period has been approved for a record category, it must be stated in the applicable retention schedule or collection-point notice and applied consistently.

Cross-border access or transfer must use a lawful mechanism and satisfy any applicable localisation, authorisation, notice, assessment, or safeguard requirement. Relevant supplier and transfer records must identify the provider, function, processing location, and applicable transfer mechanism. This Policy does not itself disclose or commit TraCerLab to a particular vendor, facility, operating architecture, storage location, or security configuration.

26.3 Confidentiality and protected disclosures

Confidentiality obligations do not prohibit a legally protected report, disclosure to a competent authority, request for legal or union advice, or participation in a lawful investigation. Nothing in this Policy requires disclosure of legally privileged material or limits a person's non-waivable rights.

27. Public claims, assurance, and reliance

TraCerLab will not make an absolute or misleading claim about compliance, effectiveness, certification, traceability, human-rights performance, absence of corruption, or absence of Modern Slavery.

Unless expressly stated in a current, scoped, and supportable assurance report:

- this Policy is not an independent certification or audit opinion;
- a Business Partner's acceptance of terms is not proof of operational compliance;
- due diligence reduces risk but does not eliminate it;
- a technical record or analytical output may be incomplete or incorrect;
- no Service guarantees detection or prevention of misconduct or harm; and
- no customer, investor, authority, or other person should treat this Policy as legal advice about its own duties.

TraCerLab may describe verified controls and outcomes accurately, including material limitations. Forward-looking commitments must be identified as plans or objectives and not as completed action.

28. Breaches, exceptions, and local implementation

28.1 Breaches

A breach may result in corrective or disciplinary action up to and including dismissal, removal from office, suspension or termination of a relationship, recovery of loss, or referral to a competent authority, subject to applicable law, contract, due process, and proportionality.

Failure to supervise, deliberate ignorance, retaliation, obstruction, false certification, concealment, or failure to escalate a known serious risk may itself be a breach.

28.2 Exceptions

There is no exception or waiver for Bribery, Kickbacks, corrupt influence, Modern Slavery, Human Trafficking, Forced Labour, or the worst forms of Child Labour.

The treatment of a payment made under genuine personal-safety duress in Section 10 is not an exception authorising the coercer's demand; it protects a person who responds reasonably to an imminent threat and then reports and records the incident as required.

Operational exceptions to a procedural control-such as an approval route or evidence format-may be granted only where:

- the underlying conduct remains lawful and consistent with the core prohibitions;
- the reason, scope, duration, risk, compensating controls, and approver are documented before action where practicable;
- Legal approves where the controlled procedure requires it; and
- the exception is recorded, monitored, and closed.

An emergency may change the timing or method of an approval but does not make prohibited conduct permissible.

28.3 Local implementation

TraCerLab may issue local addenda, work rules, codes, procedures, contract clauses, notices, or translations to implement this Policy. Local implementation must account for employee consultation, works-council, collective-bargaining, disciplinary, whistleblowing, investigation, privacy, monitoring, and translation requirements.

If a translated version conflicts with the approved English version, the English version is the reference text to the extent permitted by law; mandatory local law and a properly adopted local instrument prevail where required.

29. Policy administration and contact

Legal and Compliance maintains the controlled version of this Policy and its supporting procedures. This version takes effect only after documented approval by the Approval Authority and completion of any mandatory consultation, notice, translation, work-rule, contractual-incorporation, or other local implementation step. Approval and implementation evidence must be retained in the applicable governance record.

Before effectiveness, the Policy Owner must verify and evidence the minimum enabling controls required by this Policy, including the current risk assessment; authority and escalation map; approval matrix; gifts, hospitality, conflicts, and other required registers; Business Partner due-diligence workflow; payment controls; tested reporting routes; investigation, safeguarding, and remedy procedures; role-based training plan; privacy notices and retention rules; monitoring plan; and accountable owners. A control that is planned but not operational must not be presented as implemented, and any material implementation gap must be resolved or expressly approved, risk-assessed, time-bound, and accompanied by lawful compensating measures before release.

TraCerLab may revise this Policy to reflect changes in law, guidance, risks, Services, operations, or controls. Material changes will be approved and communicated through an appropriate channel. A change does not retroactively convert lawful past conduct into a policy breach, but continuing conduct must comply from the effective date assigned through

the approval process.

Questions, approval requests, Conflict of Interest disclosures, and concerns may be sent to:

TraCerLab Legal and Compliance

Email: legal@tracerlabgroup.com

Privacy questions and rights requests may be sent to:

TraCerLab Privacy

Email: privacy@tracerlabgroup.com

For accessibility support or an alternative format, contact either address and describe the format needed. Do not send sensitive identity documents or detailed evidence by ordinary email unless instructed through an authorised secure method.

Appendix A - Anti-bribery and corruption red flags

A red flag does not prove misconduct. It requires clarification, evidence, and risk-appropriate escalation before proceeding. Examples include:

A.1 Identity, ownership, and relationships

- ownership or beneficial ownership is hidden, inconsistent, unusually complex, or recently changed;
- a Business Partner will not identify principals, subagents, or relevant Public Official connections;
- an official, customer decision-maker, employee, or relative recommended or selected the Business Partner;
- the Business Partner has no relevant staff, premises, qualifications, or track record;
- the entity was formed shortly before the opportunity or uses nominees without a clear rationale;
- adverse information, debarment, sanctions, enforcement, or credible allegations are dismissed without evidence; or
- a conflict is undisclosed or the reviewer is pressured to ignore it.

A.2 Scope and compensation

- services, deliverables, territory, or need are vague or duplicative;
- commission, success fee, margin, rebate, discount, or expense is excessive or unexplained;
- compensation is tied to an official act, tender, permit, tax result, inspection, or regulatory decision;
- a payment is requested before work, immediately before a decision, or after an adverse outcome;
- the Business Partner claims unique influence, a special relationship, or guaranteed access;
- a side letter, oral term, sham deliverable, or artificial invoice is proposed; or
- the person refuses proportionate anti-bribery terms, records, or verification.

A.3 Payment and records

- cash, personal accounts, third-party accounts, digital assets, gift cards, or bearer instruments are requested;
- payment is routed through an unrelated country, entity, charity, consultant, or account;
- invoices use vague terms or lack evidence of completed work;
- amounts are split below an approval threshold or repeatedly rounded;
- an official fee lacks a published basis or official receipt;
- a refund, credit, petty-cash item, or personal expense is used to conceal value; or
- records are backdated, altered, withheld, or destroyed.

A.4 Conduct and pressure

- there is unusual secrecy, urgency, intimidation, or insistence that normal review be bypassed;

- a person says the payment is customary, necessary, untraceable, or approved "off the record";
- an official or decision-maker requests a gift, job, donation, trip, contract, or benefit for another person;
- access is conditioned on using a particular intermediary;
- a concern is followed by threats, demotion, exclusion, or other Retaliation; or
- a manager prioritises closing the transaction over resolving a red flag.

When a red flag appears: pause the relevant commitment or payment where safe and lawful, preserve evidence, avoid alerting a potentially implicated person, and contact Legal.

Appendix B - Business-courtesy decision rule

Before offering, promising, accepting, or arranging a business courtesy, the requestor and approver should be able to answer yes to every applicable question:

- Is the purpose legitimate, necessary, and documented?
- Is it lawful under the rules applicable to TraCerLab, the recipient, and the location?
- Is it unrelated to a pending or foreseeable decision?
- Is it reasonable, proportionate, infrequent, and not cash or a cash equivalent?
- Would it remain appropriate if publicly disclosed with the giver, recipient, value, and purpose?
- Is there no quid pro quo, request, secrecy, splitting, or use of an intermediary?
- Has the total pattern of benefits to the recipient and connected people been considered?
- Has the required written approval been obtained before commitment?
- Will the expense be paid through an authorised route and recorded accurately?
- For a Public Official, has Legal confirmed the recipient's rules and granted written approval?

If any answer is no, unknown, or dependent on concealment, do not proceed until Legal resolves it. An internal monetary threshold never overrides this test.

Appendix C - Modern-slavery and labour-risk indicators

An indicator may have an innocent explanation, and exploitation can exist without every indicator. The response must consider the full context and the safety of affected people.

C.1 Recruitment and movement

- workers paid fees, incurred unexplained debt, pledged property, or borrowed from the recruiter or employer;
- recruiters misrepresented pay, work, location, employer, accommodation, or immigration status;
- contracts were absent, substituted, untranslated, or signed after travel or work began;
- workers cannot leave accommodation, transport, a site, or employment freely;
- passports, permits, bank cards, phones, or personal documents are retained; or
- a worker is threatened with denunciation, deportation, detention, violence, or debt enforcement.

C.2 Work and pay

- wages are withheld, paid into another person's account, unlawfully deducted, or materially below the agreed amount;
- hours are excessive, involuntary, inaccurately recorded, or linked to threats;
- workers cannot take lawful rest, refuse unsafe work, resign, or access medical care;
- accommodation or food creates coercive debt or dependency;

- workers are isolated, guarded, coached, fearful, or unable to speak privately; or
- multiple workers repeat identical explanations in the presence of management or a recruiter.

C.3 Children and vulnerable people

- a worker appears below the lawful minimum age or performs hazardous work while under 18;
- age records are missing, altered, inconsistent, or collected through a discriminatory process;
- children work to repay family debt or are controlled by an adult who is not a legitimate caregiver;
- a person shows signs of violence, sexual exploitation, untreated injury, hunger, or extreme fatigue; or
- a reporter, union representative, community member, or human-rights defender faces threats after raising labour concerns.

C.4 Business and site controls

- labour is supplied through undisclosed layers, informal brokers, or unverified subcontractors;
- a site, accommodation, or workforce cannot be accessed without management selection or notice;
- records conflict with worker accounts or appear prepared only for audit;
- the price or deadline appears incompatible with lawful wages, hours, recruitment, or safety;
- corrective actions repeatedly close without worker verification; or
- workers disappear, are dismissed, or are transferred after an audit or grievance.

If there is immediate danger, prioritise safety and qualified support. Do not confront a suspected exploiter, remove a child without a safeguarding plan, promise immigration outcomes, or publish identifying information.

Appendix D - Minimum due-diligence evidence

The required evidence varies by risk, but a defensible file should ordinarily identify:

Topic	Evidence to retain where applicable
Purpose and owner	Business rationale, responsible relationship owner, scope, need, and alternatives considered
Identity and control	Verified legal identity, registration, address, ownership, beneficial ownership, management, and authorised signatories
Risk assessment	Country, sector, service, public-interface, labour, conflict, sanctions, and human-rights risks; severity and rationale
Integrity review	Qualifications, references, connections, conflicts, enforcement, debarment, credible adverse information, and explanation of findings
Commercial terms	Deliverables, pricing, commission, expenses, payment route, tax treatment, subcontracting, and reasonableness assessment
Human-rights controls	Recruitment model, workforce, worker-paid fees, document handling, grievance access, child-labour controls, safety, and remediation capability
Approvals	Reviewers, decision, conditions, residual risk, escalation, date, and expiry or refresh trigger
Contract	Applicable compliance clauses, reporting, flow-down, audit, corrective action, suspension, termination, and remediation rights
Monitoring	Deliverables, invoices, payments, incidents, certifications, worker or stakeholder feedback, corrective actions, and renewal review

A file is incomplete if a reviewer cannot understand what was known, what was checked, how red flags were resolved, why the relationship was approved, and what monitoring was required.

Appendix E - Incident-response priorities

When suspected bribery, exploitation, trafficking, severe labour abuse, or Retaliation is reported, the initial response should consider these priorities in order, adapting them to the facts:

- Immediate safety: identify urgent threats and obtain qualified emergency or safeguarding support where appropriate.
- Non-retaliation: separate or protect affected people without exposing the reporter or implying guilt.
- Independence: identify conflicts and appoint an authorised, qualified decision-maker or investigator.
- Preservation: protect relevant records, accounts, devices, payments, and physical evidence lawfully.
- Legal duties: assess mandatory reporting, privilege, employment, privacy, child-protection, trafficking, sanctions, and regulator requirements.
- Operational containment: pause a payment, access, decision, shipment, engagement, or other activity where lawful and proportionate.
- Fair investigation: define allegations, scope, evidence, interviews, rights, and communication controls.
- Remedy: involve affected people appropriately and address wages, fees, documents, safety, status, support, or other harm.
- Root cause: identify incentives, management failures, data gaps, purchasing practices, third-party weaknesses, or control circumvention.
- Governance and follow-up: report material matters, assign corrective actions, test closure, and monitor recurrence.

This sequence is a decision aid, not a substitute for professional safeguarding, legal, investigative, or emergency advice.

Appendix F - Annual statement control checklist

Before an annual modern-slavery, forced-labour, supply-chain, or due-diligence statement is approved, the preparer must document:

- the exact legal basis and scope analysis;
- the reporting entities and period;
- required content, approval, signature, publication, registry, and deadline;
- sources and owners for every material factual claim;
- reconciliation with procurement, workforce, finance, due-diligence, grievance, investigation, audit, and remediation records;
- clear separation of completed actions, ongoing work, future plans, and unavailable information;
- review for confidentiality, safety, privilege, privacy, competition, sanctions, and reporting restrictions;
- legal and responsible-function review;
- formal approval and signature evidence; and
- a retained final copy, publication evidence, and version history.

The reviewer must remove or qualify any statement that cannot be substantiated for the reporting period. A statement should explain material limitations candidly without exposing individuals, confidential counterparties, operating architecture, vendors, storage locations, or security configurations unless disclosure is legally required and approved.