Center for Implementation of Investment Projects

Framework on Prohibited Practices

2025
DUSHANBE, REPUBLIC OF TAJIKISTAN

Table of Contents

1. Introduction and Purpose

The Center for the Implementation of Investment Projects (CIIP), operating under the Committee for Environmental Protection of the Republic of Tajikistan, is dedicated to promoting sustainable development through the effective management of environmental investment projects.

In fulfilling its mandate, CIIP recognizes the critical importance of maintaining the highest standards of integrity, transparency, and accountability. Unethical conduct, including corruption, fraud, money laundering, and terrorism financing, poses significant risks to development outcomes and erodes stakeholder trust. Therefore, establishing a robust framework for identifying, reporting, investigating, and resolving prohibited practices.

The Center for the Implementation of Investment Projects (CIIP) upholds a strict zero-tolerance policy towards Prohibited Practices. CIIP is firmly committed to preventing and combating such practices across all its operations and activities.

CIIP expects all individuals and entities involved in its activities to adhere to the highest standards of integrity. This includes refraining from directly or indirectly condoning, encouraging, participating in, or engaging in Prohibited Practices. Furthermore, CIIP requires the implementation of appropriate measures to prevent and address Prohibited Practices in all its activities.

The primary objective of this Framework on Prohibited Practices is to establish a comprehensive and coherent approach to preventing, detecting, and addressing unethical conduct within the operations of the Center for the Implementation of Investment Projects (CIIP). By delineating clear definitions of prohibited practices and outlining procedures for reporting and investigation, the framework aims to uphold the highest standards of integrity, transparency, and accountability. This commitment ensures that all activities under CIIP's purview are conducted in compliance with national legislation of the Republic of Tajikistan and adhere to the stringent requirements set forth by international partners, including the Adaptation Fund and the Green Climate Fund.

2. Definitions

For the purposes of this Framework **“Prohibited Practices”** mean any of the following practices set out below:

“Corruption”: Offering, giving, receiving, or soliciting anything of value to influence the actions of another party improperly.

“Fraud”: Any act or omission, including misrepresentation, that knowingly or recklessly misleads or attempts to mislead a party to obtain a financial or other benefit or to avoid an obligation.

“**Coercion”**: Impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.

“**Collusion”**: An arrangement between two or more parties designed to achieve an improper purpose, including influencing improperly the actions of another party.
“**Obstruction”**: Deliberately destroying, falsifying, altering, or concealing evidence material to an investigation, or making false statements to investigators.
“**Retaliation Against Whistleblowers”**: Any detrimental action taken against a whistleblower or witness for reporting or participating in an investigation of prohibited practices.
“**Money Laundering**” The conversion or transfer of property, knowing it is derived from criminal activity, for the purpose of concealing or disguising its illicit origin.
“**Terrorism Financing”**: The provision or collection of funds with the intention that they be used to carry out acts of terrorism.
"Sexual Exploitation": Abuse of position or power for sexual purposes including profiting from another person's sexual exploitation.
"Sexual Abuse": Physical intrusion of a sexual nature by force or under unequal conditions.
"Sexual Harassment": Unwelcome sexual conduct that creates hostile environments, interferes with work or becomes a condition of employment.

3. Scope

This framework applies to all individuals and entities involved in the planning, execution, and oversight of projects and programs managed or supported by CIIP. This includes, but is not limited to, CIIP staff, implementing partners, contractors, consultants, and any other stakeholders engaged in CIIP-related activities.

The framework encompasses all stages of project and program cycles, from initial planning and approval through implementation and evaluation. It addresses a range of unethical behaviors, including corruption, fraud, money laundering, terrorism financing, and other practices that undermine organizational integrity. By establishing mechanisms for reporting, investigating, and resolving complaints, the framework ensures that all parties are held accountable and that whistleblowers and witnesses are protected from retaliation.

4. Legal and Regulatory Framework

The Center for the Implementation of Investment Projects (CIIP) operates within a comprehensive legal and regulatory framework that encompasses national legislation, international obligations, and the specific requirements of funding partners. This framework ensures that CIIP's operations adhere to the highest standards of integrity, transparency, and accountability.

4.1 National Legislation of the Republic of Tajikistan

This framework aligns with Tajikistan’s legal and regulatory requirements on anti-corruption, fraud prevention, and the fight against money laundering and terrorism financing. This includes

compliance with local anti-corruption laws, financial crime regulations, and whistleblower protection laws.

Key national laws include:

- Law No. 1714 "On Combating Corruption" (2020):[1] This law defines the organizational and legal framework for combating corruption and is aimed at protecting human and civil rights and freedoms. It outlines preventive measures, responsibilities of public officials, and mechanisms for public participation in anti-corruption efforts.
- Law No. 1950 "On Combating Legalization (Laundering) of Criminal Proceeds, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction" **(2023):**[2] This legislation establishes the legal basis for anti-money laundering (AML) and counter-terrorism financing (CTF) measures. It designates the Financial Monitoring Department under the National Bank of Tajikistan as the Financial Intelligence Unit (FIU) responsible for collecting and analyzing suspicious transaction reports.
- Law "On Combating Terrorism**":**[3] This law outlines the state's approach to preventing, uncovering, and responding to terrorist activities. It includes provisions for the identification and freezing of assets related to terrorism financing.
- Criminal Code of the Republic of Tajikistan (1998, as amended):[4] The Criminal Code criminalizes various forms of corruption, including bribery, abuse of power, embezzlement, and fraud. Specific articles address offenses such as illegal access (Art. 298), data interference (Art. 299), and computer-related fraud (Art. 247).
- Presidential Decree No. 143 (2018):[5] This decree validates the Regulation on the Agency for State Financial Control and Anti-Corruption, defining its mandate to prevent, detect, and investigate corruption offenses.

4.2 International Standards Compliance

This framework incorporates requirements from international funding agencies including the Adaptation Fund's Environmental and Social Policy, Gender Policy and fiduciary standards. CIIP ensures alignment with Green Climate Fund integrity policies while maintaining compliance with evolving international standards for prohibited practices prevention and environmental and social safeguards implementation.

[1] Law on Combatting Corruption

[2] Law On counteraction of legalization (washing) of income gained in the criminal way, to financing of terrorism and financing of distribution of weapons of mass destruction

[3] Law on Combatting Terrorism

[4] Criminal Code of the Republic of Tajikistan

[5] Presidential decree About Agency on the state financial control and fight against corruption of the Republic of Tajikistan

5. Guiding Principles and Objectives of the Framework

The Center for the Implementation of Investment Projects (CIIP) is dedicated to upholding the highest standards of integrity, transparency, and accountability in all its operations. This commitment is articulated through the following key principles and objectives, which guide the implementation of the Framework on Prohibited Practices:

Integrity and Accountability: CIIP emphasizes the importance of ethical conduct and responsibility. All personnel and stakeholders are expected to perform their duties with honesty and in accordance with applicable laws and regulations, ensuring that resources are used effectively and for their intended purposes.

Zero Tolerance Policy: CIIP adopts a strict zero-tolerance stance towards all forms of prohibited practices, including corruption, fraud, money laundering, terrorism financing, coercion, collusion, abuse, obstruction, and retaliation against whistleblowers. This policy aligns with the standards set by the Adaptation Fund and the Green Climate Fund, as well as national legislation such as Tajikistan's Law No. 1714 "On Combating Corruption" and Law No. 1950 "On Combating Legalization (Laundering) of Criminal Proceeds, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction."

Clear Reporting Mechanisms: The framework establishes confidential and accessible channels for reporting concerns related to unethical conduct. These mechanisms are designed to encourage stakeholders to report incidents without fear, ensuring timely and effective responses.

Whistleblower Protection: Recognizing the importance of safeguarding individuals who report misconduct, CIIP has implemented an internal Whistleblower Protection Policy. This policy ensures that whistleblowers are protected from retaliation, even in the absence of specific national legislation on whistleblower protection.

Investigative Procedures: The framework outlines thorough and impartial procedures for investigating allegations of prohibited practices. These procedures ensure that all reports are addressed systematically, respecting the rights of all parties involved.

Continuous Improvement: To maintain relevance and effectiveness, the framework is subject to regular reviews and updates. This process ensures alignment with evolving best practices, regulatory requirements, and the dynamic operational environment.

Environmental and Social Responsibility: CIIP commits to implementing projects that promote positive environmental and social benefits while avoiding, minimizing or mitigating adverse impacts. All projects are screened for environmental and social risks during design and monitored throughout implementation in alignment with the Adaptation Fund's Environmental and Social Policy.

Gender-Responsive Approaches: CIIP recognizes unique vulnerabilities of different groups to climate change impacts and ensures gender-responsive approaches in all activities. Project design and implementation actively promote women's empowerment, equal access to benefits and gender-balanced participation in decision-making processes.

6. Structure and Approach to the Framework on Prohibited Practices

CIIP's framework on prohibited practices is structured to provide a comprehensive, preventive, and responsive approach to integrity risks across all its operations and project activities. The framework is operationalized through a set of dedicated policies and procedures, each detailed in a corresponding annex and aligned with international standards and national legislation.
The structure includes the following components:

- **Anti-Corruption Policy (Annex 1)** outlines measures to prevent, detect, and address acts of corruption such as bribery, kickbacks, and conflicts of interest. It includes provisions for ethical training, due diligence, and enforcement mechanisms.
- **Anti-Fraud Policy (Annex 2)** defines fraudulent conduct and sets out controls to detect and investigate fraud, with accessible reporting mechanisms and clearly defined sanctions.
- **Anti-Money Laundering Policy (Annex 3)** introduces procedures to monitor financial transactions, identify suspicious activity, and ensure compliance with AML regulations through due diligence, reporting, and staff training.
- **Counter-Terrorism Financing Policy (Annex 4)** aims to prevent the misuse of CIIP resources for terrorism financing. It provides a risk-based approach to partner screening, monitoring, and secure reporting of suspicious behavior.
- **Policy on the Protection of Whistleblowers and Witnesses and Complaint Mechanism (Annex 5)** guarantees protection from retaliation for those who report unethical behavior or assist in investigations, and establishes multiple, confidential reporting channels.
- **Investigation Guidelines and Procedures (Annex 6)** provide step-by-step instructions for managing internal investigations into allegations of prohibited practices. The annex ensures impartiality, confidentiality, and clarity on consequences and corrective measures.
- **Policy on Prevention and Response to Sexual Exploitation, Abuse, and Harassment (SEAH) (Annex 7)** establishes CIIP's comprehensive approach to preventing and responding to all forms of sexual misconduct within its operations and funded activities. The Policy recognizes that sexual exploitation, abuse and harassment constitute serious violations of human rights and fundamental breaches of the trust placed in development organizations.

Together, these annexes form an integrated framework that supports CIIP's commitment to transparency, accountability, and zero tolerance for corruption and unethical behavior.

7. Delivery and Implementation of the Framework

To ensure the effectiveness of CIIP's Framework on Prohibited Practices, dedicated efforts will be made to operationalize its components across the institution. Implementation will be guided by the principles of awareness, accountability, and institutional alignment.

7.1 Training and Awareness

CIIP establishes comprehensive training programs ensuring all personnel and partners understand prohibited practices obligations while developing effective prevention and response capacity. Training programs are tailored to different roles and responsibilities while maintaining consistent standards across organizational levels and operational contexts.

Training design reflects the best international practices and incorporates lessons learned from sector experience and organizational incidents. Programs combine theoretical knowledge with practical skills development while addressing cultural competency and context-specific challenges arising in different operational environments.

Mandatory training components include foundation courses covering all prohibited practices categories within 30 days of engagement, specialized SEAH prevention incorporating scenario-based learning, anti-corruption awareness featuring case studies and money laundering prevention focusing on transaction monitoring. Whistleblower protection familiarization and investigation procedures training support comprehensive capacity development across relevant personnel categories.

Role-specific programs provide enhanced training for managers covering response obligations and escalation procedures, specialized investigator certification incorporating trauma-informed techniques, community engagement training addressing cultural sensitivity and procurement staff development covering corruption risks and due diligence requirements. Finance team training focuses on suspicious activity identification while partner organization programs cover compliance requirements and capacity building support.

Training delivery combines in-person workshops, online learning modules and peer learning sessions with interactive exercises promoting practical skill development. External expert sessions address specialized topics while regular effectiveness evaluation through participant feedback and knowledge assessment supports continuous improvement. Training content updates reflect lessons learned, policy changes and evolving international standards with quality assurance ensuring consistent delivery across all organizational contexts.

7.2 Communication and International Cooperation

CIIP maintains transparent communication channels while participating in international cooperation mechanisms that strengthen sector-wide integrity. These arrangements recognize that prohibited practices transcend organizational boundaries and require coordinated institutional responses.

Internal communication ensures timely policy updates and compliance information reach all personnel through official channels, briefings and training sessions. External cooperation facilitates information sharing with peer organizations while maintaining appropriate confidentiality protections for sensitive investigations.

International cooperation includes participation in cross-debarment agreements with development finance institutions, information sharing on substantiated violations and coordination on due diligence procedures. Regular consultation with funding agencies ensures alignment with evolving standards while contribution to sector databases supports collective prevention efforts.

Cross-debarment procedures require systematic checking of international lists before partner engagement, prompt reporting of sanctions to relevant networks and recognition of peer institution decisions following appropriate due process. Secure databases document integrity violations and facilitate information sharing within established confidentiality frameworks.

7.3 Monitoring and Reporting

CIIP will implement an internal system to monitor the implementation of the framework and track compliance. This system will include:

- A registry of all reported cases of prohibited practices;
- Documentation of investigation outcomes and corrective actions;
- Periodic compliance reviews by the Internal Audit Unit;
- Annual reporting to CIIP senior management and donors on implementation progress and trends.

8. Monitoring and Evaluation (M&E)

A robust M&E system will be established to assess the performance, relevance, and outcomes of the framework on prohibited practices.

8.1 Evaluation Framework

CIIP will develop a formal evaluation approach that includes:

- Feedback collection from staff and implementing partners on usability and effectiveness;
- Inclusion of framework performance indicators in external audits and internal reviews;
- Evaluation checklists or scorecards to assess compliance at project and institutional levels.

8.2 Continuous Improvement

The framework will be subject to periodic review (at least biennially) to ensure alignment with:

- Evolving legal requirements at national and international levels;
- Lessons learned from investigations or audit findings;
- Emerging risks or institutional changes.

Recommendations from evaluations, audits, and stakeholder feedback will be used to update policies and implementation procedures.

8.3 Impact Assessment

CIIP will track the long-term effectiveness of the framework in reducing incidents of prohibited practices. Impact metrics may include:

- Reduction in the number or severity of substantiated cases;
- Improvement in staff awareness and risk reporting rates;
- Increased trust among stakeholders in CIIP's integrity systems.

Where feasible, impact will be assessed using baseline and comparative data to demonstrate progress over time.

8.4 Public Reporting and Transparency

CIIP maintains appropriate transparency regarding integrity efforts while protecting individual confidentiality and sensitive investigation information. This approach balances public accountability requirements with privacy protections and operational security considerations essential for effective prohibited practices prevention.

Transparency commitments reflect funding agency requirements and stakeholder expectations while contributing to broader sector learning and accountability. Public reporting focuses on aggregate trends, systemic issues and institutional improvements rather than individual case details that could compromise privacy or ongoing investigations.

Annual integrity reporting includes aggregate statistics on incidents and outcomes, trend analysis covering risk factors and prevention effectiveness, capacity building activity summaries and framework assessment identifying improvement areas. Financial impact analysis encompasses recovered funds, investigation costs and prevention investments with stakeholder communication covering funding agency reporting and public disclosure through organizational channels.

Reporting safeguards ensure all information appears in anonymized aggregate form protecting individual privacy while legal review confirms compliance with confidentiality requirements. Consultation with affected parties occurs where appropriate before sensitive information disclosure with regular protocol updates reflecting best practices and stakeholder feedback.

Stakeholder communication encompasses regular funding agency reporting as required by agreements, governance body submissions for accountability purposes and public report availability through organizational websites. Participation in sector reporting initiatives and benchmarking exercises with peer organizations supports comparative analysis while proactive communication about policy updates and lessons learned enhances transparency and sector learning.

9. Budget and Resource Allocation

Effective delivery of the framework requires adequate resourcing and institutional commitment.

9.1 Budget

CIIP will allocate specific budget lines for:

- Development and rollout of training programs;
- Operation of reporting and case management systems;
- Investigation activities and external legal support;
- Awareness-raising campaigns and stakeholder engagement.

These costs will be included in CIIP's annual operational planning and donor-funded project proposals.

9.2 Staffing

Dedicated personnel will be assigned to oversee framework implementation, including:

- A Compliance Officer or Integrity Focal Point;
- Internal audit and legal support staff;
- Designated investigators for complex or sensitive cases.

Staff will receive specialized training and technical tools to perform their duties effectively.

9.3 External Resources

Where internal capacity is limited, CIIP may engage:

- Independent experts for forensic investigations or legal reviews;
- External trainers to deliver targeted workshops;
- Partner organizations with expertise in compliance and ethics systems.

Annex 1: Anti-Corruption Policy

1. Purpose and Objective

The purpose of this Anti-Corruption Policy is to establish a comprehensive framework for the prevention, detection, and response to corruption within the Center for Implementation of Investment Projects (CIIP). It aims to ensure that CIIP upholds the highest standards of integrity, transparency, and accountability in accordance with:

- The Law of the Republic of Tajikistan "On Combating Corruption[6]";
- The Law "On Public Service"[7];
- The Criminal Code[8] (provisions related to bribery, fraud, and abuse of authority);
- And international standards, including the United Nations Convention against Corruption (UNCAC).

2. Definitions

For the purposes of this policy, the following terms are defined as:

- **Corruption**: The abuse of entrusted power for private gain, including bribery, extortion, embezzlement, and other forms of dishonest or fraudulent behavior.
- **Bribery**: Offering, giving, receiving, or soliciting something of value as a means to influence the actions of an official or other person in a position of authority.
- **Kickback**: A form of bribery where a portion of funds is returned to the payer as a reward for facilitating a transaction or contract.
- **Facilitation Payment**: A small, unofficial payment made to expedite routine government action, which is considered a corrupt practice under this policy.
- **Conflict of Interest**: A situation where an individual's personal interests may compromise their duties and decision-making for CIIP.
- **Whistleblower**: Any individual who reports suspected wrongdoing, fraud, or corruption in good faith, and is entitled to protection against retaliation.

3. Scope of Application

This policy applies to all:

- CIIP employees, consultants, interns, and contractors;
- Implementing partners and beneficiaries involved in CIIP-funded projects;
- External stakeholders interacting with CIIP in a business or regulatory capacity.

4. Core Principles

CIIP adopts a zero-tolerance approach to corruption and commits to:

- Full compliance with national anti-corruption laws and public service codes;

[6] Anticorruption Law
[7] Law on Public service
[8] Criminal Code

- Transparent operations and procurement processes;
- Integrity in project appraisal, fund disbursement, and contract management;
- Timely reporting, impartial investigation, and disciplinary enforcement.

5. Prevention Measures

CIIP believes that **prevention is the most effective way to combat corruption**. To that end, the organization adopts proactive measures designed to reduce the risk of unethical behavior across all levels of operation. These measures include legal compliance, education and awareness, and strong internal control systems.

5.1. Legal Compliance and Institutional Governance

CIIP ensures that all its operations are fully compliant with relevant national anti-corruption legislation and the requirements of international development partners. Oversight bodies within CIIP, such as the **Legal Division** and **Internal Audit Unit**, are responsible for embedding anti-corruption principles into internal policies, reviewing adherence to legal standards, and facilitating regular updates.

5.2. Staff Training and Awareness

Awareness is key to prevention. CIIP provides mandatory training to all new and existing staff on corruption risks, national legal obligations, institutional codes of conduct, and ethical decision-making. These sessions emphasize the importance of acting with integrity and reporting any suspected misconduct promptly.

5.3. Risk-Based Due Diligence

CIIP applies comprehensive risk-based approaches to managing corruption and integrity risks across all partnerships and transactions. Different activities, partners and contexts present varying risk levels requiring tailored due diligence measures proportionate to identified exposure.

Enhanced screening procedures include systematic verification against international sanctions lists, terrorist designation databases and cross-debarment networks maintained by development organizations. Criminal background checks are conducted where legally permitted with reference verification focusing on conduct and integrity issues.

Comprehensive background verification encompasses financial vetting through audited statements and tax records, legal entity verification including beneficial ownership structures, and institutional capacity assessment covering governance arrangements and implementation experience. Site visits and physical verification are conducted for significant partnerships or high-risk contexts.

Risk-based decision making applies standard procedures for low-risk activities while implementing enhanced measures for complex ownership structures and significant financial

exposures. Clear escalation procedures ensure senior management review for high-risk findings with comprehensive documentation of decisions and mitigation measures in partner files.

Ongoing monitoring includes regular re-screening based on risk classifications, transaction monitoring for unusual patterns and updated assessments reflecting changing circumstances. Contractual safeguards incorporate anti-corruption clauses, audit rights and immediate termination provisions for integrity violations.

6. Reporting, Whistleblower Protection, and Investigation

A culture of accountability relies on clear, safe, and confidential mechanisms for reporting concerns.
CIIP maintains an accessible **Grievance Redress Mechanism (GRM)** that allows internal and external parties to report suspicions of corruption or unethical conduct. This system includes online and in-person channels and ensures **anonymity and protection against retaliation** for whistleblowers.

Upon receiving a report, CIIP will:

- Acknowledge and register the complaint;
- Conduct a **preliminary assessment** to determine credibility;
- Carry out an **impartial investigation**, involving the Internal Audit Unit and, if necessary, external legal counsel;
- Document findings and recommend corrective action or escalation to national authorities.

Whistleblower protection is guaranteed under the **Law "On Combating Corruption"** of Tajikistan and CIIP's internal procedures. Individuals who report in good faith will not face disciplinary measures or retaliation.

7. Enforcement and Sanctions

CIIP is committed to ensuring that breaches of anti-corruption policies are addressed decisively and transparently. Disciplinary actions for confirmed violations will follow due process and be proportionate to the severity of the offense.

Enforcement mechanisms include:

- **Administrative measures**: such as written warnings, demotion, or suspension;
- **Contractual remedies**: such as contract cancellation or financial restitution by third parties;
- **Legal escalation**: including reporting to the **Agency for State Financial Control and Combating Corruption** and cooperating fully with criminal investigations.

This ensures that CIIP does not merely identify corruption but actively **punishes and deters** it through structured, legally sound procedures.

8. Monitoring, Review, and Continuous Improvement

CIIP recognizes that anti-corruption efforts must be **dynamic and adaptive** to remain effective. As such, the organization is committed to **regularly monitoring the implementation of this policy**, assessing its relevance, and updating it in line with emerging risks, legal changes, and global best practices.

8.1. Monitoring Compliance

- The **Internal Audit Unit/relevant specialist**, in coordination with the **Legal Division/Lawyer**, will oversee periodic reviews of financial transactions, procurement activities, and project implementation processes to ensure they comply with anti-corruption standards.
- Audit findings and risk assessments will inform management decisions on improving controls and minimizing exposure to corruption.

8.2. Annual Review and Policy Updates

- The Anti-Corruption Policy will undergo a **formal review at least once per year**, or sooner if triggered by:
    - Amendments to national anti-corruption laws;
    - New guidance or requirements from development partners;
    - Lessons learned from internal investigations or audits.
- Revisions will be approved by senior management and, if applicable, submitted to relevant government oversight bodies for alignment with national strategies.

8.3. Learning and Capacity Enhancement

- CIIP will use findings from internal audits, stakeholder feedback, and case studies to **enhance internal capacity**, update training materials, and adapt procedures.
- Participation in national and international **anti-corruption networks or platforms** will be encouraged to exchange knowledge, benchmark practices, and adopt innovative tools.

By institutionalizing continuous improvement, CIIP strengthens its position as a **transparent and accountable organization**, upholding the trust of donors, government authorities, and the public.

9. Environmental and Social Compliance Integration

Anti-corruption measures extend to environmental and social safeguard implementation preventing fraud in impact assessments, consultation processes and benefit distribution. Enhanced due diligence includes verification of environmental and social compliance while monitoring encompasses safeguard implementation effectiveness assessment.

Annex. 2 Anti-Fraud Policy

1. Purpose and Objective

Fraud poses a serious threat to the integrity, resources, and credibility of public institutions. The objective of this policy is to ensure that CIIP has the systems and culture in place to prevent, detect, and respond to fraudulent activities effectively and consistently. The policy supports CIIP's commitment to ethical conduct, proper use of resources, and full compliance with applicable laws, including the Law of the Republic of Tajikistan on Combating Corruption.

2. Scope

This policy applies to:

- All CIIP employees, consultants, contractors, and implementing partners;
- All CIIP-funded projects and programs;
- All stakeholders engaged in financial or operational transactions with CIIP.

The policy covers all forms of **fraudulent activity**, including but not limited to:

- **Financial fraud**: theft, embezzlement, falsification of accounting records, and manipulation of financial data;
- **Misrepresentation**: providing false information to secure funding, contracts, or other benefits;
- **Misuse of resources**: unauthorized or improper use of CIIP's assets, materials, or services for personal gain.

3. Definitions

The following definition are used for the purpose of this policy:

- **Fraud**: Any intentional act or omission designed to deceive others, resulting in financial or personal gain for the perpetrator and loss or risk for CIIP.
- **Financial fraud**: The manipulation or misstatement of financial records to gain an undue advantage.
- **Misrepresentation**: The intentional provision of false or misleading information.
- **Asset misuse**: The unauthorized use or appropriation of CIIP's funds, property, or services.
- **Internal control**: Mechanisms put in place to prevent or detect errors, mismanagement, or fraud.

4. Principles

The guiding principles of this policy are rooted in CIIP's **zero-tolerance stance toward fraud**. The organization believes that fraud prevention is not only a legal obligation but also a moral imperative for building trust with funders, government agencies, and the public.

These principles include:

- Integrity and accountability at all levels;
- Transparent systems and decision-making processes;

- Prompt and fair responses to suspected fraud;
- Alignment with national and international standards for fraud prevention.

5. Preventive Measures

CIIP adopts a proactive approach to **fraud prevention** through the implementation of the following measures:

5.1. Internal Controls

- Clear separation of duties in procurement, financial transactions, and approval chains;
- Use of dual authorizations and verification for payments;
- Secure documentation and record-keeping protocols.

5.2. Regular Audits

- Internal and external audits will be conducted periodically to identify anomalies, verify compliance, and assess control effectiveness;
- Audit results will inform improvement of procedures and risk management strategies.

5.3. Staff Training

- Regular training on anti-fraud awareness, red flags, and reporting obligations will be provided to all personnel;
- Special sessions for finance, procurement, and project staff to enhance detection capacity.

6. Reporting Mechanisms

CIIP fosters a culture where individuals feel safe and supported in reporting suspected fraud.

- CIIP's GRM will include fraud reporting options with clear confidentiality guarantees;
- Staff and stakeholders may report anonymously or by name through secure email, phone, or submission boxes;
- All reports will be received in good faith and processed through an impartial procedure.

These mechanisms ensure that reporting is accessible, protected, and encouraged across the organization.

7. Investigation and Response

Once a credible report of fraud is received, CIIP will:

- Assign qualified internal or external investigators;
- Conduct fair, thorough, and timely investigations;
- Document findings and take appropriate corrective measures.

Where criminal conduct is confirmed, CIIP will cooperate with the relevant national authorities, including the Agency for State Financial Control and Combating Corruption, ensuring that violators are held accountable in accordance with the law.

8. Enforcement and Disciplinary Action

Enforcement ensures that the policy is not just a guideline but a standard of accountability. If fraud is proven, consequences may include:

- Termination of employment or contractual engagement;
- Recovery of misappropriated funds or assets;
- Referral for prosecution under the Criminal Code of Tajikistan;
- Public or donor disclosure, where required.

The application of sanctions will follow due process, ensuring fairness while maintaining a deterrent effect.

9. Monitoring and Review

CIIP will ensure that this policy remains relevant and effective by:

- Reviewing it at least annually;
- Updating it in response to audit findings, new laws, or evolving fraud risks;
- Benchmarking against peer institutions and engaging in training or forums on fraud prevention.

Monitoring implementation helps build a culture of continuous improvement and institutional learning, ensuring that CIIP remains compliant and resilient.

Annex 3. CIIP Anti-Money Laundering (AML) Policy

1. Purpose and Objective

The purpose of this Anti-Money Laundering Policy is to establish clear and consistent procedures to **prevent, detect, and report money laundering activities** within CIIP operations. Money laundering presents a serious risk to financial integrity, and this policy ensures that CIIP's systems and controls are aligned with the national legal framework and international standards, including the **Law of the Republic of Tajikistan on Combating Legalization of Criminally Acquired Incomes and Financing of Terrorism**, and relevant FATF (Financial Action Task Force) guidelines.

The objective is to:

- Prevent CIIP from being used—intentionally or unintentionally—as a conduit for laundering illicit funds;
- Protect the institution's credibility and financial transparency;
- Strengthen compliance and mitigate reputational and legal risks.

2. Scope

This policy applies to:

- All CIIP **staff, consultants, contractors, and project partners** involved in financial transactions;
- All projects financed, managed, or overseen by CIIP, regardless of funding source;
- All external entities conducting business with CIIP.

It covers:

- Monitoring and verification of financial flows;
- Due diligence in beneficiary and partner selection;
- Detection of and response to **unusual or suspicious financial activity**.

The wide scope ensures comprehensive protection and **prevention across all CIIP operations**, leaving no vulnerable point for misuse of financial resources.

3. Definitions

To ensure clarity and consistent application, the following key terms are defined:

- **Money Laundering**: The process of disguising the origins of money obtained through illegal means to make it appear legitimate.
- **KYC (Know Your Customer)**: A set of procedures used to verify the identity of clients and partners before entering financial relationships.

- **Suspicious Transaction**: Any activity or pattern of transactions that appears inconsistent with expected behavior and could indicate criminal intent.
- **Beneficial Owner**: The natural person who ultimately owns or controls a legal entity or is the ultimate recipient of a transaction.
- **Enhanced Due Diligence**: A deeper investigation into high-risk clients or transactions, requiring more extensive documentation and monitoring.

These definitions ensure that **staff at all levels use a common language and understanding** when applying the policy.

4. Compliance Measures

CIIP will implement specific compliance tools and procedures designed to uphold AML requirements across its operational framework.

4.1. Know Your Customer (KYC)

CIIP requires that **each project partner, grantee, or service provider** undergo identity verification before entering a financial relationship. KYC procedures include:

- Collection of legal entity documents, licenses, and tax registrations;
- Verification of the **beneficial ownership structure**;
- Cross-checking against watchlists, sanctions lists, and databases for politically exposed persons (PEPs).

This ensures CIIP **knows who it is dealing with** and reduces the risk of being exploited for illicit purposes.

4.2. Due Diligence

Due diligence is a key AML control. CIIP will:

- Apply **standard due diligence** for low-risk activities;
- Apply **enhanced due diligence** for higher-risk cases, such as offshore transactions or opaque organizational structures.

Due diligence ensures that CIIP only partners with entities that demonstrate legal compliance and ethical behavior.

4.3. Recordkeeping

CIIP will keep full records of:

- Partner verification documents;
- Transaction histories;
- Correspondence related to KYC and risk classification.

All records will be **retained for at least five years** in line with Tajik law and international AML best practices.

5. Monitoring and Detection

CIIP will maintain **ongoing surveillance** of its financial flows to identify unusual or potentially suspicious activity. This includes:

- Reviewing project disbursements, payment justifications, and supplier contracts;
- Monitoring for patterns such as:
    - Repeated transactions just below thresholds;
    - Sudden changes in transaction destinations;
    - Payments to high-risk jurisdictions.

This allows CIIP to act proactively and **intervene before serious breaches occur**.

6. Reporting Requirements

When red flags or suspicious transactions are identified, CIIP has a legal and institutional obligation to act promptly and responsibly to prevent potential misuse of funds or involvement in illicit financial activities.

6.1 Mandatory Reporting Obligation

All CIIP staff—regardless of position or seniority—are required to **immediately report** any suspected or observed instance of money laundering, attempted concealment of funds, or irregular financial activity.

6.2 Submission Process:

Reports must be submitted **directly and confidentially** to the designated **AML Compliance Officer** or other **Relevant Responsible Person** appointed within CIIP.

Reports can be submitted in **written form (email or physical form)** using a standardized **Suspicious Activity Report (SAR)** template, or through an **internal secure reporting channel** (e.g., confidential email inbox, dedicated reporting form on CIIP's intranet).

Where available, **anonymous reporting** will also be allowed through a secure, password-protected online reporting system to protect whistleblowers.

All reports must include factual details such as the nature of the concern, dates, individuals or entities involved, and any relevant supporting documents.

6.3 Confidentiality and Protection:

All reports are treated as **strictly confidential**. Only authorized personnel involved in the investigation (e.g., Compliance Officer, Legal Counsel) will have access to report details.

The identity of the reporting individual will be protected in accordance with CIIP's **Whistleblower Protection Policy**. Retaliation against anyone who reports in good faith is strictly prohibited and may result in disciplinary action.

6.4 Documentation and Escalation:

Upon receipt of the report, the AML Compliance Officer will log the report in a secure registry, assess its validity, and, if necessary, **escalate the case to senior management and/or national authorities** such as the Financial Monitoring Center (FMC).

All actions taken in response to the report will be documented to maintain an **audit trail** for internal review or donor oversight.

These reporting procedures ensure that CIIP fulfills its **legal, ethical, and fiduciary responsibilities** under both national anti-money laundering laws and the compliance frameworks of development partners and climate finance entities (e.g., Adaptation Fund, Green Climate Fund).

6.5 Roles and Responsibilities of the AML Compliance Officer

The **AML Compliance Officer** plays a central role in implementing and enforcing the Anti-Money Laundering Policy at CIIP. The officer is appointed by senior management and must operate with independence, authority, and access to relevant information.

Key Responsibilities:

1. **Policy Oversight and Implementation**
    - Ensure that AML procedures are effectively integrated into CIIP's operations, finance, procurement, and project implementation processes.
    - Regularly update the AML Policy based on changes in law, donor requirements, and emerging risks.
2. **Monitoring and Due Diligence**
    - Oversee KYC and due diligence processes, particularly for high-risk transactions or partners.
    - Review transaction records, flag anomalies, and recommend enhanced scrutiny where necessary.
3. **Investigation of Reports**
    - Receive, document, and assess all Suspicious Activity Reports (SARs) submitted by staff.
    - Conduct preliminary investigations while maintaining confidentiality and due process.
    - Escalate confirmed cases to appropriate authorities, including the Financial Monitoring Center or donor compliance units.

4. **Record-Keeping and Audit Support**
    - Maintain a secure log of all reports, actions taken, and outcomes.
    - Support internal and external audits related to AML compliance and provide requested documentation.
5. **Training and Awareness**
    - Organize regular training sessions for staff on AML regulations, reporting mechanisms, and red flag indicators.
    - Serve as a point of contact for questions, advice, or clarification regarding suspicious behavior or AML risks.
6. **Reporting to Management**
    - Provide quarterly and ad hoc reports to CIIP senior management and the Internal Audit Function summarizing AML efforts, risks identified, and compliance gaps.

7. Training and Awareness

AML compliance is only effective when staff are informed and vigilant. CIIP will:

- Conduct **mandatory onboarding training** on AML risks and procedures;
- Provide **annual refresher sessions** for all staff;
- Deliver targeted training for staff in finance, procurement, and program operations.

By institutionalizing training, CIIP helps ensure that all employees are **confident and capable of identifying risks** and acting appropriately.

8. Review and Updates

This policy will be:

- **Reviewed every two years** or earlier if required by regulatory or operational changes;
- Updated based on audit recommendations, national law amendments, or donor policy shifts;
- Overseen jointly by the **Legal Division and Finance Unit**, who will coordinate changes and ensure organization-wide dissemination.

Annex 3.1. Suspicious Activity Report (SAR) Template

Section	Description
1. Report Submitted By	
Full Name	

Position/Department	
Contact Information (optional if submitted anonymously)	
2. Date of Report Submission	DD/MM/YYYY
3. Nature of Suspicious Activity	☐ Unusual transaction pattern☐ Incomplete or inconsistent documentation☐ Reluctance to provide information☐ Use of shell or front companies☐ Sudden large or complex financial transfers☐ Other (please specify): _____
4. Description of Concern	Describe the activity or behavior observed. Include dates, amounts, entities or persons involved, and any supporting facts. Use additional pages if needed.
5. Supporting Documentation	List any attached documents (emails, contracts, invoices, bank statements, etc.):
6. Action Already Taken (if any)	Describe any steps taken so far, including discussions, refusals, or verbal explanations received.
7. Confidentiality Acknowledgement	☐ I understand this report will be handled confidentially. ☐ I request anonymity.
Signature (if not anonymous)	_____
Date	_____

Annex 4. Counter-Terrorism Financing (CTF) Policy

1. Objective

The purpose of this policy is to prevent the financing of terrorism through the resources, operations, and partnerships of the Center for Implementation of Investment Projects (CIIP). CIIP is committed to ensuring that its financial flows and project activities are not misused to support individuals, groups, or entities associated with terrorism. As part of this commitment, CIIP will take all reasonable measures to detect, deter, and report any actual or suspected cases of terrorist financing, in line with national legislation and international obligations.

This policy reinforces CIIP's zero-tolerance stance on terrorism and its dedication to maintaining high standards of institutional integrity, donor trust, and public accountability.

2. Scope

This policy applies to all individuals and entities engaged in CIIP-funded projects and programs. This includes CIIP staff, consultants, implementing partners, suppliers, contractors, sub-recipients, and any financial intermediaries operating under CIIP's oversight. The scope of the policy covers all phases of the project lifecycle, including project preparation, partner selection, procurement, disbursement of funds, and monitoring of results. The policy also applies to any external entities that receive financial or in-kind support from CIIP and are therefore subject to compliance obligations.

The policy ensures that appropriate procedures are in place to identify, evaluate, and manage the risk that CIIP resources may be diverted for the purpose of financing terrorism—whether intentionally or unintentionally.

3. Risk Management

CIIP shall adopt a risk-based approach to counter-terrorism financing, aligned with international standards such as those outlined by the Financial Action Task Force (FATF). This includes assessing and mitigating the risks of terrorism financing across all CIIP programs, transactions, and partner engagements.

To manage these risks effectively, CIIP will:

- Conduct initial and periodic risk assessments to identify project areas, sectors, or regions that may be more vulnerable to terrorist financing;
- Implement screening procedures to ensure that CIIP does not work with individuals or entities listed on relevant sanctions or terrorist designation lists (e.g., United Nations Security Council Sanctions List, national terrorism lists);

- Apply enhanced due diligence measures in higher-risk contexts, including the requirement of additional background checks, source of funds verification, and more frequent monitoring;
- Review project proposals and partner credentials with a view to identifying any red flags or inconsistencies that may indicate terrorism financing risks.

All risk management procedures will be documented and subject to internal oversight and periodic review.

4. Reporting Mechanisms

CIIP will ensure that all staff and associated personnel are aware of their duty to report any suspected or confirmed terrorism financing incidents. A clear and secure internal reporting system will be established to support timely action.

Reports must be submitted to the designated CTF Compliance Officer through secure and confidential channels. Reporting options will include:

- A designated internal email address managed by the CTF Compliance Officer;
- A standardized Suspicious Activity Report (SAR) form available to all staff;
- An anonymous reporting mechanism to protect the identity of whistleblowers where necessary.

Upon receipt of a report, the CTF Compliance Officer shall promptly assess the matter and, if warranted, initiate an internal inquiry. When suspicion is substantiated, the case will be escalated to the appropriate national authorities, including the Financial Monitoring Center of Tajikistan or relevant law enforcement bodies. All reports and investigations will be logged, securely stored, and subject to follow-up as needed.

CIIP will also encourage external parties, such as contractors and implementing partners, to report suspicious activities related to project financing through accessible communication channels.

5. Compliance

CIIP is fully committed to adhering to all national and international laws and regulations related to countering the financing of terrorism. This includes:

- The Law of the Republic of Tajikistan on Combating the Legalization of Proceeds from Crime and Financing of Terrorism;
- Relevant UN Security Council Resolutions (e.g., UNSCR 1373 and subsequent CTF resolutions);

- Conditions set forth by international development partners, including the Adaptation Fund (AF), Green Climate Fund (GCF), and other multilateral organizations.

All contracts, partnership agreements, and procurement documents issued by CIIP shall include clauses requiring full compliance with counter-terrorism financing laws. Failure to comply with this policy or related laws will result in disciplinary measures, including termination of employment or contractual relationships, in addition to potential referral to competent national authorities for legal action.

6. Capacity Building and Governance

To effectively implement this policy, CIIP shall ensure that all staff and relevant stakeholders receive appropriate training and awareness-raising on terrorism financing risks. Training will cover:

- Legal and institutional obligations regarding CTF;
- Methods of identifying suspicious activity or high-risk partners;
- Procedures for secure and confidential reporting;
- Understanding of national and international terrorist designation lists and sanctions regimes.

CIIP will designate a **CTF Compliance Officer** to oversee the implementation of this policy. The officer will be responsible for:

- Coordinating training and awareness-raising;
- Managing the screening of partners and beneficiaries;
- Receiving and investigating reports of suspicious activity;
- Serving as a liaison with national authorities and donor agencies;
- Preparing periodic reports to CIIP's senior management and the internal audit function on the organization's compliance with this policy.

The policy shall be reviewed and updated periodically to ensure continued effectiveness and alignment with legal requirements and donor standards.

Annex 4.1 – CTF Risk Screening Checklist

This checklist is used during partner selection**,** project appraisal**,** procurement, and fund disbursement to identify and assess potential terrorism financing risks.

Category	**Risk Indicator**	**Yes/No**	**Remarks / Action Required**
Legal Status & Background	Is the entity/individual properly registered and legally authorized to operate?	☐ / ☐	
	Are ownership structures transparent and verifiable?	☐ / ☐	
	Are any key persons associated with the entity listed on international or national terrorism watchlists?	☐ / ☐	Conduct sanctions screening
Geographic Risk	Does the project operate in a region identified as high-risk or conflict-affected?	☐ / ☐	Apply enhanced due diligence
	Are any project beneficiaries or partners located in jurisdictions with weak CTF controls?	☐ / ☐	Refer to FATF lists
Financial Risk	Are there unexplained or disproportionate funding sources in project proposals?	☐ / ☐	Request supporting documentation
	Are there large or complex cash-based transactions planned?	☐ / ☐	Monitor and justify
Operational Risk	Does the partner have weak internal controls or governance structures?	☐ / ☐	Request improvement plan or refuse funding
	Is there a history of suspicious activity, fraud, or other compliance violations?	☐ / ☐	Require disclosure or legal clearance

Instructions*: Any "Yes" responses require detailed review and documentation. If more than two high-risk indicators are present, escalate the case to the CTF Compliance Officer for enhanced due diligence or rejection.*

Annex 4.2 – Suspicious Activity Report (SAR) Template for CTF

Confidential – Counter-Terrorism Financing Suspicious Activity Report (SAR)
(To be completed by CIIP staff or associated personnel)

1. Reporter Information

- Name:
- Department/Unit:
- Position:
- Contact Information:

2. Date and Time of Report Submission

- Date: ___ / ___ / _____
- Time (if applicable):

3. Details of Suspicious Activity

- Description:

Please describe the suspicious behavior or incident, including dates, involved individuals or organizations, and any unusual financial transactions observed. Attach documents if applicable.

- Type of Suspicion (tick all that apply):
☐ Link to designated terrorist organization
☐ Use of unverified intermediaries
☐ Large/unusual cash payments
☐ Suspicious changes to payment instructions
☐ High-risk geographic location
☐ Anonymous donations or untraceable funds
☐ Other (please specify):

_____
_____
_____
_____

4. Supporting Documentation

List and attach relevant evidence, such as emails, invoices, partner files, or transaction records.
_____
_____
_____

5. Requested Confidentiality

☐ I request that my identity remain confidential
☐ I am submitting this report anonymously

6. Signature (if applicable)

Signed: _____
Date: ___ / ___ / _____

Annex 5. Policy on the Protection of Whistleblowers and Witnesses and Complaint Mechanism

1. Objective

The objective of this Policy is to ensure the protection of individuals affiliated with CIIP who, in good faith, report suspected misconduct or participate as witnesses in related investigations. CIIP is committed to fostering a culture of transparency, accountability, and integrity by providing secure avenues for reporting and ensuring that whistleblowers and witnesses are safeguarded from retaliation, discrimination, or any form of harm.

2. Scope

This Policy applies to all CIIP employees, consultants, implementing partners, contractors, suppliers, project beneficiaries, and any other stakeholders engaged in CIIP-funded or implemented projects and activities. It covers:

- Whistleblowers who report concerns related to fraud, corruption, abuse of authority, harassment, financial mismanagement, environmental or social safeguard violations, or breaches of national or donor regulations;
- Witnesses who provide information during internal inquiries or external investigations.

3. Reporting Channels

CIIP will ensure that accessible, confidential, and secure channels are available for submitting complaints and disclosures. These include:

- A confidential email managed by CIIP's Internal Audit Unit;
- An online grievance submission form available on CIIP's website https://tajciip.org to enable anonymous or named complaints from internal and external parties.;
- A sealed written complaint addressed to the CIIP Director or designated Whistleblower Protection Officer;
- In-person or phone reporting to designated focal points, including Gender, E&S, or Safeguards Officers who can record and escalate concerns.

CIIP will handle all reports in a manner that guarantees confidentiality and data protection, in compliance with applicable laws and internal regulations. CIIP prohibits the sharing of information beyond those directly involved in the investigative process.

4. Protection Measures

CIIP shall implement the following protection measures to ensure the safety and rights of whistleblowers and witnesses:

- **Prohibition of retaliation:** Any form of reprisal, intimidation, demotion, or discrimination as a result of reporting will not be tolerated.

- **Temporary protective arrangements:** Where necessary, CIIP may implement measures such as reassignment, flexible working arrangements, or leave of absence to protect individuals.
- **Disciplinary action against retaliators:** Individuals who engage in retaliatory behavior will face appropriate disciplinary consequences.
- **Access to support services:** Whistleblowers and witnesses may receive legal, psychosocial, or security assistance where risk or distress is evident.
- **Confidential handling of complaints:** Documentation is securely stored and only accessible to authorized personnel, ensuring protection of identities and sensitive information.

Protection applies even if the reported concern is not substantiated, provided the disclosure was made in good faith.

5. Investigation Guidelines and Procedures

To uphold fairness and integrity, CIIP follows a structured process for investigating all eligible complaints.

5.1 Objective

To establish a transparent, consistent, and impartial methodology for investigating allegations of misconduct or prohibited practices. Investigations aim to uncover the truth while ensuring due process and accountability.

5.2 Scope

The investigation procedures apply to allegations involving:

- **Corruption, bribery, and fraud:** Including misuse of funds, falsified documents, or procurement irregularities;
- **Money laundering and terrorism financing:** Including the use of project funds to support unlawful financial activity;
- **Sexual misconduct and abuse of power:** Violations of dignity, exploitation of vulnerable persons, and abuse in workplace or field operations;
- **Environmental and social harms:** Breaches of safeguard standards that negatively impact project-affected communities or ecosystems;
- **Other unethical or unlawful practices** identified during the course of CIIP's operations.

These procedures apply across all project sites, partnerships, and levels of CIIP's institutional structure.

5.3 Investigation Process

- **Step 1: Intake and Preliminary Review**
  CIIP's Internal Audit Unit/ Whistleblower Protection Officer, or designated authority, receives the complaint and conducts an initial review to determine admissibility, credibility, and relevance. Cases deemed admissible proceed to formal investigation.
- **Step 2: Formal Investigation**
  Investigators collect evidence through interviews, document reviews, and on-site assessments. All parties are treated fairly, and the investigation follows CIIP's Code of Conduct and relevant national laws. Investigators declare any conflicts of interest and operate independently.
- **Step 3: Findings and Reporting**
  Investigation results are compiled in a written report, detailing findings, substantiations, and recommendations. The report is submitted to senior management or CIIP's Audit Committee for review and decision-making.
- **Step 4: Resolution and Follow-Up**
  CIIP implements corrective or disciplinary actions, as appropriate, based on the investigation's conclusions. The whistleblower or witness may be informed of the outcome, within the bounds of confidentiality.

5.4 Confidentiality and Fairness

CIIP is committed to ensuring that all investigations are conducted with the highest standards of integrity, confidentiality, and procedural fairness. Respecting the rights and dignity of all parties involved—whistleblowers, witnesses, and alleged respondents—is essential to maintaining trust in the complaint mechanism and ensuring the legitimacy of the investigative process. CIIP applies a victim-centered, survivor-sensitive, and impartial approach in all investigations, in line with international best practices and donor standards.

- The following principles guide the conduct of investigations:
- **Confidentiality:** Information related to the complaint and investigation is shared strictly on a need-to-know basis. The identity of whistleblowers and witnesses is protected throughout the process unless they consent to disclosure or where disclosure is required by law.
- **Non-retaliation:** CIIP enforces a strict prohibition on retaliation against any individual who reports concerns or participates in an investigation. This includes protection from dismissal, demotion, intimidation, harassment, or any adverse action.
- **Impartiality:** Investigators are required to maintain objectivity, independence, and neutrality. Any real or perceived conflicts of interest are disclosed and managed appropriately to preserve the integrity of the process.
- **Respect for rights:** All parties have the right to be informed of relevant proceedings, to present information or respond to allegations, and to be treated fairly and respectfully during interviews or other interactions.

5.5 Outcomes and Consequences

Following the completion of an investigation, CIIP will determine appropriate outcomes based on the findings and recommendations outlined in the investigation report. These outcomes aim to ensure accountability, deter future misconduct, and strengthen institutional systems and controls. The nature and severity of the consequence will be proportionate to the gravity of the offense, the extent of the impact, and whether the conduct involved intentional wrongdoing.

Possible outcomes include:

- **No further action**, if allegations are not substantiated by the investigation and no breach is found.
- **Corrective actions**, such as strengthening internal procedures, improving staff training, or modifying workflows to prevent recurrence.
- **Administrative or disciplinary sanctions**, which may include verbal or written warnings, suspension, demotion, reassignment, or termination of employment or contract.
- **Referral to external authorities**, including law enforcement or regulatory agencies, when criminal conduct or regulatory breaches are suspected.
- **Disclosure to donors or oversight bodies**, as required under the terms of donor agreements or national laws.

CIIP ensures that all actions taken are documented and communicated to the appropriate internal and external stakeholders while maintaining necessary confidentiality. Outcomes will also inform institutional learning and be integrated into future risk mitigation and compliance planning.

6. Follow-Up and Investigation

Upon receipt of a complaint or disclosure:

- CIIP Whistleblower Protection Officer will conduct a preliminary review to assess its validity and urgency;
- If warranted, a formal investigation will be launched by Whistleblower Protection Officer or an appointed independent investigator;
- The whistleblower or witness will be kept informed, where appropriate, about the status and resolution of the case;
- Any substantiated violations will result in appropriate corrective measures, disciplinary actions, or legal proceedings;
- Lessons learned will be incorporated into institutional risk management, ethics training, and compliance procedures.

7. Oversight and Review

CIIP's Whistleblower Protection Officer/Internal Audit Unit will be responsible for the implementation and monitoring of this Policy. Periodic reviews will be conducted to ensure continued alignment with national legislation, donor requirements (including the Green Climate Fund, Adaptation Fund, and others), and international standards on whistleblower protection. The Policy shall be publicly disclosed and disseminated to all CIIP personnel and stakeholders through orientation sessions, internal communication channels, and official documentation.

8. Victim and Survivor Support Services

CIIP recognizes that individuals affected by prohibited practices require comprehensive support extending beyond retaliation protection to encompass medical, psychological, legal and practical assistance. This commitment reflects international standards emphasizing victim-centered approaches and organizational responsibility for addressing misconduct-related harm.

Support services address immediate crisis needs and longer-term recovery requirements while respecting individual autonomy and cultural preferences. Service delivery combines direct provision where feasible with referral arrangements and financial support for accessing specialized external providers.

Immediate support encompasses emergency medical care, crisis counseling, safe accommodation arrangements, legal consultation and practical assistance including transportation and interpretation services. Medium-term support includes continued mental health services, legal representation for formal proceedings, temporary financial assistance and flexible work arrangements for organizational personnel.

Long-term recovery support provides ongoing counseling access, career development opportunities, skills training programs and community reintegration assistance. Regular follow-up and case management ensure continued service access with needs assessment and effectiveness monitoring supporting service quality assurance.

Service coordination mechanisms include direct provision through organizational resources, partnership agreements with specialized providers, referral networks with pre-established arrangements and financial support for external service access. Quality assurance encompasses regular provider evaluation, cultural competency requirements and survivor feedback integration into service improvement processes.

ANNEX 6. Investigation Guidelines and Procedures

1. Purpose

This annex sets out the procedures and standards for conducting impartial, timely, and thorough investigations into allegations of prohibited practices within CIIP. These include corruption, fraud, collusion, coercion, terrorism financing, money laundering, sexual exploitation, abuse, harassment (SEAH), and other forms of misconduct.

The purpose is to ensure that all reported incidents are treated seriously and that investigations are carried out in a fair, consistent, and confidential manner, protecting both the integrity of the process and the rights of all parties involved.

2. Applicability

These procedures apply to all CIIP personnel, including staff, consultants, contractors, implementing partners, and third parties engaged in CIIP-financed activities. The guidelines cover both internal complaints and reports submitted by external stakeholders, including through grievance redress or whistleblower channels.

3. Guiding Principles

- **Confidentiality**: All information related to investigations is to be handled with strict confidentiality. Disclosure of information will be limited to those with a need to know.
- **Impartiality**: Investigations will be conducted without bias, with investigators avoiding actual or perceived conflicts of interest.
- **Timeliness**: Investigations should be initiated promptly after a complaint is received and concluded without undue delay.
- **Due Process**: All parties will be given the opportunity to be heard, to respond to allegations, and to present evidence.
- **Protection Against Retaliation**: CIIP will protect individuals who report misconduct in good faith from retaliation or reprisal.

4. Investigation Process

4.1. Receipt and Preliminary Review

- Complaints or allegations must be submitted in writing, verbally, or anonymously through secure reporting channels (e.g., email, internal forms, whistleblower hotline to be found in CIIP's official website).
- The CIIP **Compliance or Integrity Officer** will conduct a preliminary review within 5–10 working days to assess credibility and relevance.
- If the complaint falls outside the scope of CIIP's mandate, it will be referred to the appropriate authority or agency.

4.2. Case Registration and Assignment

- Valid cases are registered in the Confidential Case Registry and assigned a unique reference number.
- The **Compliance or Integrity Officer** designates a qualified investigator or investigation team based on the nature and sensitivity of the allegation.

4.3. Planning and Notification

- An Investigation Plan is developed, outlining the scope, methodology, timelines, and information required.
- The subject(s) of the investigation will be formally notified of the investigation, unless such notice would compromise the inquiry or safety.

4.4. Evidence Collection and Interviews

- Investigators will gather relevant documentation (e.g., emails, reports, financial records) and conduct interviews with witnesses, complainants, and respondents.
- Interviews will be recorded (with consent) and documented to maintain an audit trail.

4.5. Analysis and Findings

- The investigation team will assess the facts against applicable CIIP policies, national laws, and donor standards.
- Findings will be classified as:
    - Substantiated
    - Partially Substantiated
    - Unsubstantiated
    - Inconclusive

4.6. Investigation Report and Recommendations

- A formal Investigation Report will be prepared, summarizing evidence, findings, and any recommended actions.
- The report is submitted to CIIP senior management and/or relevant disciplinary committee for decision-making.
- Where applicable, findings will be shared with donors or external authorities.

5. Outcomes and Resolution

Following the investigation:

- Disciplinary actions may include warnings, suspension, contract termination, legal action, or recovery of funds.
- Systemic weaknesses identified may lead to policy or process improvements.
- In cases involving criminal conduct (e.g., terrorism financing, money laundering), the matter will be referred to national law enforcement bodies.

Where the complaint is not substantiated, no adverse actions shall be taken against the accused. However, CIIP reserves the right to take preventive measures where necessary.

6. Monitoring and Closure

The **Compliance or Integrity Officer** will monitor the implementation of corrective actions and close the case once actions are completed and documented. A summary of key investigations (without disclosing personal data) may be included in periodic internal reports or donor updates.

7. Information Sharing and Cross-Debarment Coordination

CIIP participates in international cooperation mechanisms designed to prevent movement of sanctioned individuals and entities between organizations while contributing to collective sector learning on prohibited practices prevention.

Cross-debarment obligations require notification to relevant networks within 30 days of final disciplinary decisions with necessary documentation provided while protecting sensitive investigation details. Legal coordination ensures compliance with data protection requirements while maintaining comprehensive records of all communications and network participation activities.

Recognition of external debarment decisions includes regular database checking before partner engagement, immediate implementation of recognized sanctions and establishment of appropriate appeal procedures. Documentation requirements ensure consistent application with legal and compliance team coordination supporting policy implementation.

Information sharing activities encompass participation in anonymized trend analysis, contribution to sector research initiatives and collaboration with academic institutions on integrity innovation. Regular consultation with funding agencies and oversight bodies supports policy development while sharing best practices through professional networks enhances collective prevention capacity.

Annex 7: Policy on Prevention and Response to Sexual Exploitation, Abuse, and Harassment (SEAH)

1. Purpose and Objective

This Policy establishes CIIP's zero-tolerance approach to Sexual Exploitation, Abuse and Harassment in all operations and funded activities. The policy ensures protection for personnel, partners, beneficiaries and communities while meeting international standards required by funding agencies.

CIIP recognizes that SEAH violates human rights and undermines organizational integrity. This policy provides frameworks for prevention, reporting, investigation and response to ensure accountability and safe environments.

2. Scope

This policy applies to all CIIP personnel, implementing partners, contractors and beneficiaries. Coverage includes all CIIP-funded activities and interactions with project-affected populations across all operational contexts.

3. Definitions

Sexual Exploitation means abuse of position or power for sexual purposes. Sexual Abuse means physical intrusion of a sexual nature by force or under unequal conditions. Sexual Harassment means unwelcome sexual conduct that creates hostile environments or interferes with work. Child means any person under 18 years. Survivor-Centered Approach means prioritizing survivor rights and decisions in all responses.

4. Prohibited Conduct

CIIP maintains zero tolerance for all forms of SEAH. Sexual activity with children under 18 years is absolutely prohibited. Sexual exploitation or abuse of beneficiaries and community members is forbidden. Sexual harassment in any work context is not permitted. Exchange of money, goods or services for sexual activity constitutes a serious violation.

5. Prevention Measures

All personnel must sign comprehensive Codes of Conduct prohibiting SEAH with clear consequences for violations. CIIP conducts background screening including criminal checks where legally permitted and reference verification with conduct inquiries. Mandatory SEAH training occurs within 30 days of engagement covering policy requirements, reporting mechanisms and survivor-centered approaches. Annual refresher training is required for all personnel.

6. Reporting and Response

CIIP provides confidential reporting channels including dedicated hotlines, online systems and in-person options. Personnel have mandatory duties to report SEAH concerns immediately with enhanced responsibilities for managers. External reporting to law enforcement and funding agencies occurs when required.

Upon receiving reports, CIIP ensures survivor safety, implements protection measures and conducts thorough investigations using trained investigators. Interim measures including suspension may be applied during investigations.

7. Support for Survivors

CIIP provides immediate support including medical care, crisis counseling, safe accommodation and legal consultation. Ongoing support encompasses mental health services, legal representation, financial assistance and community reintegration support. Services are delivered through direct provision, specialized partnerships and referral arrangements.

8. Disciplinary Actions

Substantiated violations result in appropriate sanctions ranging from warnings to termination. Criminal conduct is referred to law enforcement with full cooperation provided. Disciplinary information is shared with cross-debarment networks and other organizations to prevent rehiring of offenders.

9. Protection from Retaliation

Retaliation against reporters, witnesses and survivors is strictly prohibited. CIIP provides confidentiality protections, security measures and alternative arrangements to ensure safety. Swift action is taken against retaliatory conduct.

10. Implementation and Monitoring

CIIP designates senior-level focal points with operational oversight responsibilities. Adequate resources are allocated for prevention, investigation and support activities. Regular monitoring tracks incidents, training effectiveness and policy implementation. Annual public reporting provides aggregate statistics while protecting individual confidentiality.

Partnerships with specialized service providers, government agencies and international organizations enhance prevention and response capacity. Policy improvements are made based on implementation experience and evolving international standards.